INSTITUTIONALIZED ENVIRONMENTS AND INFORMATION SECURITY MANAGEMENT: LEARNING FROM Y2K

A Comparative Study in a Critical Sector Organization

A Dissertation
Presented to
The Academic Faculty

by

Pamela Grace Burns Hassebroek

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy in the
School of Public Policy

Georgia Institute of Technology
August 2007

INSTITUTIONALIZED ENVIRONMENTS AND INFORMATION SECURITY MANAGEMENT: LEARNING FROM Y2K

A Comparative Study in a Critical Sector Organization

Approved by:

Dr. Juan D. Rogers, Advisor
School of Public Policy
Georgia Institute of Technology

Dr. Hans K. Klein
School of Public Policy
Georgia Institute of Technology

Dr. Jay D. Bolter
School of Literature, Communication, & Culture
Georgia Institute of Technology

Mr. Mike Nelson-Palmer
College of Computing
Georgia Institute of Technology

Dr. Gordon Kingsley
School of Public Policy
Georgia Institute of Technology

Date approved: June 13, 2007

A … model for improving security may be the *Y2K* bug. Facing the threat of widespread computer meltdowns at the millennium, industry mobilized to change business practices and governments passed laws requiring *Y2K* certification for tech gear. Companies underwent massive campaigns to make certain they complied because they didn't want to be held liable for damages. The Securities & Exchange Commission required corporations to provide details of their *Y2K* efforts in quarterly earnings reports.

—Sager, I., & Greene, J., Business Week

If we could do it this time, why not do it next time and every time? In many companies, success with *Y2K* could become the role model for success in all future IT [information technology] projects.

—Yourdon, E., Computerworld

ACKNOWLEDGEMENTS

My success in designing and writing this dissertation reflects the contributions of many individuals, from both inside and outside organizations, who offered information, advice, encouragement, funding, inspiration, hope, and friendship during the Ph.D. process. Individuals from a number of departments at Georgia Tech imparted the educational foundation that led to this degree: the School of Public Policy, the College of Computing, the School of Literature, Communication and Culture, and the Office of Graduate Studies and Research.

In the School of Public Policy, members of the faculty and fellow students have contributed immeasurably both to my education and in guidance for this research. Thanks to all of you for your generous contributions. Juan Rogers, chair of my dissertation committee, served as a willing and competent advisor on many occasions when I needed critical direction during the dissertation process. He directed the development of the research protocol for the Institutional Review Board, and assisted me in honing the research design. His advice has been invaluable to the completion of this dissertation. Hans Klein also provided essential direction for which I am especially grateful. Hans served as my advisor through the initial stages of my research—advising me in narrowing the topic of information security, in framing the literature, and in helping me to understand the value of "theory." The study of *Y2K* was his idea. Gordon Kingsley, another valued member of my committee, introduced me to the field of public policy; his able leadership for the class entitled *Scope and Theory of Public Policy* inspired me to join the Ph.D. program. Susan Cozzens, another significant contributor from the School,

served as a faithful counselor throughout my journey in the Ph.D. program. Officially, Susan served as academic advisor and as my employer in research assistantships. Unofficially, she was always available to help as I attempted to plot a route through various aspects of the program, giving thoughtful consideration to my questions, even as she attended to her far-reaching research agenda and either chairing the department or directing the Ph.D. program. Latissia Caldwell-Jones, graduate coordinator, was so valuable both to me and to the functioning of the graduate programs in the School that I would find it difficult to rule out her hand in any aspect. She made it happen! Her interpersonal skills, her winning personality, and her willingness to tackle almost any graduate student issue all added joy to the transactions involved in accruing the requirements for the Georgia Tech degree. I also acknowledge the good fortune in the collegial support of fellow Ph.D. students and friends, especially Dara, Jingjing, Min, and Carolyn. Thank you for being there, and for patiently listening to many versions of my "evolving" theories and strategies and for offering feedback on my early and ill-formed presentations.

In the Georgia Tech College of Computing (CoC), where I spent an interim course of study, Sy Goodman and Mike Nelson-Palmer were responsible for my early education in the field of information security. Sy served as first advisor for this dissertation, and suggested the direction for my research topic area—information security in organizations. My experiences working under Sy's direction were important and rewarding; and, I am very grateful for his mentoring. I also appreciate the myriad opportunities that he provided for me to contribute to the field. Thanks to Sy, I was able to develop course content, write for presentation and publication, assist in teaching, and

to connect with the field of information security through conferences and meetings, where practitioners and policy-makers were discussing real-world problems. Thank you also to Mike Nelson-Palmer, manager of the Georgia Tech Information Security Center (GTISC). Mike skillfully taught the CoC course that served as my introduction to the study of information security. In addition, as a member of my dissertation committee, he provided extensive and important feedback on this document. I also recognize the contribution of Peter Wan, information security technical expert, a former employee in the CoC and later in the Georgia Tech Office of Information Technology. Peter provided opportunities to discuss the evolution of IT systems and security processes. David McCann and Ben Garrison, CoC students, provided assistance in computer programming and data organization. Thank you to all of these CoC contributors.

In the School of Literature, Culture, and Communication, Jay Bolter was thesis advisor for my Master's research, as well as a member of my Ph.D. dissertation committee. He led classes exploring the "new media," which included the World Wide Web and virtual reality. Thank you, Jay, for the instruction and early mentoring, for your loyalty and continued support. Anne Balsamo, head of the graduate program, was also a valued committee member for my Master's work. Her course in communication theory and culture was an important influence in my dissertation research.

The writing workshops in the GT Office of Graduate Studies and Research were very helpful when I first began to struggle with the notion of "academic writing." Amanda Gable read a number of early drafts of various sections of my writing, and gave me encouragement along the way with valuable feedback. Amanda's support and her faithful friendship have been a wonderful addition to my life at Georgia Tech. Many,

many thanks to you, Amanda. Thank you also to Georgia Tech students Tim Hartman and Nancy McKee, who contributed considerably to this research by assisting me in organizing and analyzing documents.

Beyond the boundaries of Georgia Tech, individuals associated with Delta were critical to the importance of this research. The Delta community—employees and consultants, past and present—has been an exceptionally generous group to work with, especially those individuals who offered personal time to provide data, to help me navigate among the Delta divisions, organizational relationships, and, most especially, to help me understand its technical jargon. Leo Mullin, along with Walter Taylor, Tim Mitchell, Charlie Feld, Charles Gravitt, Gerald Grinstein, Neal Morgan, Curtis Robb, John Day, Jack McMillan, and numerous others have contributed to this research, thus personifying the supportive family that the Delta organization is known to be. I owe an enormous debt of gratitude to all of you; I could not have accomplished this dissertation without your contribution.

In addition to the abovementioned support for my academic work, a constellation of professionals has contributed significantly to my ability to sustain focus and energy for this dissertation. I have been very blessed to know and to be in the care of extraordinarily knowledgeable and effective practitioners in their respective fields; it is impossible to overestimate the value of these "angels" in my life. First from Emory University, Nadine Kaslow served as trustworthy and conscientious mentor, counselor, and coach, and more recently as text editor. Thank you, Nadine, for your dedication. The leaders and members of the Dissertation Support Group at Georgia Tech, and the Cancer Support Group at the Samaritan Counseling Center, also provided a supportive environment at times when I

greatly needed it. Trisha Senterfitt and Nancy Kirwan demonstrate an inspiring and extraordinary calling. Next, over these years of long days of computer work, my physical therapists helped me to maintain stamina and balance. Melissa Wirsig, Peter Hergott, and Jayne Edwards applied their expertise to improve my physical condition beyond what I had ever considered possible. Finally, George Wirth, spiritual and behavioral exemplar and my friend, never failed to believe that I could accomplish the doctoral degree, calling me "soon to be Dr." at every meeting since I began the Ph.D. program. George and Barb are wonderful friends; and I extend a hand to them especially for the hope that they instill in so many.

I also had the blessing of the continuous encouragement of my family, both past and present. I often think of my parents. Even though they are no longer here to witness my achievement, I feel their presence and remember their educational endeavors and their love of learning. I am certain that it is to them that I owe my greatest debt. They would have been extremely proud. I also remember my brother Reed, a man with a brilliant mind who seemed to know something about everything. Brain cancer took his life during my comprehensive exam process. Since then I have so often wished I could discuss my research ideas and topics with him; I know that he would have contributed immeasurably to my understanding. My children Carter and Katherine have been trusting supporters from the beginning, unfailingly believing that I would attain my degree. Along the way, I added a daughter-in-law, Katie, and three grandchildren, Jessica, Nolan, and Ellie, all of whom have inspired me to discipline my time so that I could get to know them better. However, my sister Carla has done the most to elevate my energy and my

standing throughout the Ph.D. process! She is my active fan, my lifelong companion, and most faithful friend. I therefore owe her a public thank you for being there for me.

Last but of course, not least, my husband Jerry has been physically the closest to my work and has sacrificed the most personally to enable this dissertation. I am extremely grateful for his handling of many asset management duties (read: cooking and bill paying) during these years of my research and writing. His assistance was provided following retirement from his 30-year career as a partner in Andersen Consulting (now Accenture), an event that came in my second year of the Ph.D. program. While at Accenture, he witnessed first hand the evolution of popular management concepts, and the transformation of information systems in organizations. His recall and insights regarding those experiences have been an invaluable aid to this research.

Finally, I received support for preparation of this dissertation in part by funds from the U.S. Department of Defense, Cisco Systems, the International Information Systems Security Certification Consortium [ISC]^2, and from the Georgia Tech School of Public Policy, for which I am sincerely grateful.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

TERMINOLOGY AND DEFINITIONS

In order to stabilize various uses of terms throughout the Delta documentation, this list serves to define and / or clarify terminology for purposes of this research. Official definitions are excerpted from a number of sources.[1]

A&P license	Airframe and Powerplant License The A&P license, issued by the FAA, certifies aircraft mechanics for performing maintenance operations. The airframe is the aircraft body; the powerplant is the engine.
AAAC	Airlines Airport Affairs Committee AAAC refers to a group that facilitates cooperative arrangements between airlines and airports. (AAAC is a generic term.)
ACARS	Aircraft Communications Addressing and Reporting System ACARS is a datalink system that enables ground stations (airports, aircraft maintenance bases, etc.) and commercial aircraft to communicate data, such as fuel quantity, weight on wheels, FMS, etc.
ACAS	Airborne Collision Avoidance Systems ACAS is an electronic means for detecting other aircraft, designed to help avoid midair collisions. The ACAS provides a backup to visual search and the ATC system. However, threat aircraft must be equipped with an ICAO-compliant altitude reporting transponder, not universally required as of 2007.
ACC	Airport Coordination Center The ACC is the main tactical command center for daily operation in Delta's hubs and strategic stations, providing support for local station operation, and coordination with the OCC/ATL. ACC employees are responsible for coordination, communication, service delivery, and recovery to Delta's passengers when unexpected irregularities arise.
ACI-NA	Airports Council International - North America ACI-NA is the largest of the six worldwide regions of Airports Council International (ACI), an organization of airports worldwide. ACI-NA airport members enplane 95% of all domestic and virtually all international airline passenger and cargo traffic in North America. ACI-NA promotes cooperation with the commercial civil aviation industry in order to exchange ideas, information, and experiences on common airport issues. (http://www.aci-na.org/).

[1] Airline industry-specific terms from Jones (1998), Delta Air Lines (2006), and websites of airline industry and government organizations. Information security terms from "Glossary of Key Information Security Terms," (2006).

ACM	Asset Compliance Management ACM was the process for tracking, controlling, and monitoring of assets through the four phases of Delta's Year 2000 program. It was the process that determined if an asset was *Y2K* ready, and for those items found not ready, the process for getting them ready (Delta archive, 1998, p. 2).
ACP	Airline Control Program ACP was renamed "Transaction Processing Facility" (TPF). See TPF.
ACS	Airport Customer Service ACS is the Delta business area that included the following activities: airport ticketing, skycap services, gate and boarding processes, loading and unloading of aircraft, baggage service, cabin cleaning, cargo handling and shipping, pre-board security screening, and the ACC at hubs (ramp tower).
ADIZ	Air Defense Identification Zone The U.S. and Canada jointly administer the ADIZ, which is almost entirely over water. The area serves as a national defense boundary for air traffic over North America. Any aircraft flying in or through the boundary must have filed either a Defense Visual Flight Rules (DVFR) flight plan or an Instrument Flight Rules (IFR) flight plan before crossing the ADIZ.
ADS-B	Automatic Dependent Surveillance-Broadcast An ADS-B signal broadcasts directly from aircraft, enabling the location of aircraft by a 1090 MHz receiver.
AFA-CWA	Association of Flight Attendants, CWA (AFL-CIO) The AFA-CWA (affiliated with the Communications Workers of America) is the world's largest labor union (over 55,000 flight attendants at 20 airlines), and organized by flight attendants for flight attendants. AFA represents flight attendants at their workplace, in the industry, in the media and on Capitol Hill. The goal of AFA-CWA is to negotiate better pay, benefits, working conditions, and work rules for flight attendants at their respective airlines, and to improve safety on the job (http://www.afanet.org/).
AFL-CIO	American Federation of Labor-Congress of Industrial Organizations The AFL-CIO is a voluntary federation of American unions. The membership of the AFL-CIO organization comprises fifty-two unions, and represents more than 9 million workers nationwide.
ADA	Airline Deregulation Act: signed into law by President Carter in 1978. The ADA amended the Federal Aviation Act of 1958, and was designed to encourage the development of an air transportation system that relies on a competitive market to determine quality, variety, and price of services.
Airport systems	The infrastructure systems that control basic operations of an airport. Computer-based airport systems included bag/mail sort, elevators, loading bridges, HVAC, and fuel management.
ALAR	Approach-and-Landing Accident Reduction Airlines, air traffic services, and aviation authorities cooperate to improve safety and increase ALAR.

ALPA	Air Line Pilots Association, International ALPA is the largest airline pilot union in the world (62,000 pilots who flew for 39 U.S. and Canadian airlines). Founded in 1931, ALPA was chartered by the AFL-CIO and the Canadian Labour Congress. Known internationally as US-ALPA, it is a member of the International Federation of Air Line Pilot Associations (IFALPA) (http://www.alpa.org).
AMP	Aviation Millennium Project AMP was the *Y2K* program for the ATA in Washington. AMP compiled information for the use of 102 North American airlines, as well as 500 airports, pertaining to 9,000 computer dependent systems ranging from baggage systems to airport runway lights. The project had a two-year budget of $16 million.
AMT	Aircraft Maintenance Technician In 2006, Delta employed over 10,000 AMTs in Technical Operations, Delta's maintenance and repair division. (http://www.topix.net).
AOC	Airport Operating Committee See AAAC.
AOPA	Aircraft Owners and Pilots Association AOPA is a U.S. non-profit organization, membership consisting mainly of general aviators. AOPA's purpose is "to serve the interests of its members as aircraft owners and pilots, and to promote the economy, safety, [and] utility … of flight in general aviation aircraft" (http://www.wikipedia.org).
APHIS	Animal Plant and Health Inspection Service APHIS is an operating unit of the U.S. Department of Agriculture (USDA). Its mission is to protect the health and value of American agriculture and natural resources (http://www.aphis.usda.gov).
Application system	Software for a computer-based system (not an operating system). At *Delta Technology*, an application system is a collection of software that together serves to support the specific needs of a functional activity in the Delta Air Lines organization.
Apollo /Galileo	A proprietary GDS A GDS is computer-based airline reservation system (CRS) with global reach, designed for travel agents, travel suppliers, and corporations. See CRS**.**
ARC	Airlines Reporting Corporation ARC is an airline-owned financial transaction processing company.
ARINC	ARINC, originally Aeronautical Radio, Incorporated ARINC serves as the airline industry's sole licensee and coordinator of radio communications outside of the government.

ARTCC Air Route Traffic Control Center

ARTCCs are government facilities employing controllers that help to monitor air space and prevent collisions. In 1997, 20 ARTCCs were located around the country, each employing 300 to 700 controllers, with more than 150 on duty during peak hours at the busiest facilities (http://www.bls.gov/oco/ocos108.htm).

ASA Aviation Security Alliance

The ASA is an alliance within the airline industry and National Safety Council's (NSC) International Air Transport Section.

ASA Atlantic Southeast Airlines, Inc.

ASA is a regional carrier. Delta held a 24% stake in the company before selling to SkyWest in 2005.

ASD Aircraft Situational Display

ASD emits an electronic signal that enables location of aircraft operating under Instrument Flight Rules. FAA receives the data and reports it slightly delayed.

ASM Available Seat Mile

ASM is a method of tracking fares according to what a passenger paid (in cents) per mile. ASM includes several factors including purchase date, class, destination, flight date and time, fuel costs, competitors' fares, and special factors. Another factor that affects ticket pricing is the hub system itself. If a large airline controls many of the gates at an airport, passengers flying on that airline could experience higher ticket prices (http://govinfo.library.unt.edu).

ASN Aviation Safety Network

The Aviation Safety Network is a private, independent initiative that provides information on accidents and safety issues with respect to airliners, military transport planes, and corporate jets. Founded in 1996 and online since Jan 1996, the ASN Safety Database contains detailed descriptions of over 10,700 incidents, hijackings, and accidents.

ASRS Aviation Safety Reporting System (ASRS)

ASRS is a collection of 27 data sets vital to aviation safety. NASA maintains ASRS for the FAA.

ASSE American Society of Safety Engineers

ASSE is the oldest and largest professional safety organization in the U.S. Founded in 1911; its more than 30,000 members manage and consult on safety, health, and environmental issues in industry, insurance, government, and education (http://www.asse.org/).

ASTA The American Society of Travel Agents

ASTA is the world's largest association of travel professionals. Its mission is "to enhance the professionalism and profitability of members worldwide through effective representation in industry and government affairs, education and training and by identifying and meeting the needs of the traveling public" (http://www.astanet.com).

ATA	Air Transport Association of America, Inc. The ATA is the U.S. airline industry's chief lobbying group and represented the airline industry on major aviation issues before Congress, federal agencies, state legislatures and other governmental bodies. The organization promotes safety by coordinating industry and government safety programs, and serves as a focal point for industry efforts to standardize practices and enhance the efficiency of the air transport system (http://www.airlines.org).
ATAC	Air Transport Association of Canada See ATA.
ATC	Air Traffic Control ATC is a vast network of people and equipment that coordinates the movement of air traffic to make certain that planes stay a safe distance apart. Their immediate concern is safety, but controllers also direct planes efficiently to minimize delays. Some regulate airport traffic through designated airspaces; others regulate airport arrivals and departures. Controllers are certified by the FAA.
ATCA	Air Traffic Control Association ATCA is a professional organization that promotes the advancement of aviation and air traffic control. ATCA is unique in representing the spectrum of civil-military cooperation typical of global flying activities.
ATI	Antitrust immunity The U.S. Department of Transportation regulates alliances among air carriers, with a focus on how ATI affects competition and what the airlines could accomplish without it.
Atlantic Excellence	A global alliance formed in 1996 among Delta, Austrian, Sabena, and Swissair Atlantic Excellence was created via an antitrust exemption by the US DOT in June 1996 (Delta Air Lines, 1997).
ATM	Air Traffic Management A global ATM system was formed with the assistance of ICAO, and the cooperation of States, providers of air navigation services, and airspace users.
ATM	Asynchronous Transfer Mode ATM is a network technology for both local and wide area networks that supports real-time data, voice, and video communications. ATM is widely used as a backbone technology in carrier networks and large enterprises.
ATPCO	Airline Tariff Publishing Company ATPCO collects airline fare and fare related data from more than 500 airlines and distributes it to global distribution systems (GDS) (such as Amadeus/System One, Galileo, Sabre, and Worldspan) and computer reservation systems (CRS). ATPCO creates efficiencies in the process by permitting each airline to submit its information via ATPCO, thereby giving each CRS/GDS the opportunity for a single source of fare-related data.
ATP	Air Transport Pilot An ATP is a license that permits commercial aircraft operation by airline pilots.

ATS	Air Traffic Systems ATSs are systems that manage and control air traffic.
ATSA	Aviation and Transportation Security Act (ATSA): signed into law by President Bush in 2001. ATSA called for the creation of TSA within the DHS, transferring responsibility for airport security screening that had been under the FAA.
Baseline	A formal review point in the lifecycle of a computer system. Following an initial evaluation, a baseline serves as the basis for further development; and changes to a system require formal approval. During Delta's Year 2000 Program, baseline tests reflected the existing code in its existing environment, and established data to be used after renovation for the *Y2K* bug (Delta archive, dt147).
BCP	Business Continuity Planning BCP is the activity related to strategies for making certain that an organization can continue to operate in the case of failures of infrastructure services or other contingencies.
BDM	BDM, International Delta hired consultants from BDM, Inc, a multinational information technology company, to assist with *Y2K* conversion issues.
Black-McKellar	The Black-McKellar Act: signed into law by President F. D. R. in 1934. The Black-McKellar law authorized annual airmail contracts to private airlines and created a Federal Aviation Commission to recommend aviation policy. Airmail contracts were authorized at lower rates and with clauses to force separation of airlines and airplane manufacturers and to give smaller airlines a chance. In practice, the "Big Four" airlines reorganized and retained most of the airmail contracts.
BPM	Business Process Management BPM tools are software applications that help managers organize resources in terms of processes (http://www.bptrends.com).
BPM	Business Portfolio Manager The BPM was a position within the Year 2000 Program charged with administering and coordinating one of the four business areas from the "business" side as opposed to the "technology" side of Delta. The four Delta functional business areas were *Airport Customer Service*, *Operations*, *Business Support*, and *Revenue*.
BPO	Business Portfolio Owner Within the *Delta Technology* organization, software systems were grouped into four "portfolios," which corresponded to Delta functional business areas: *Airport Customer Service*, *Operations*, *Business Support*, and *Revenue*. The BPO was the individual, usually a senior management-level officer, who was responsible for the final decisions concerning Year 2000 Program solutions in a Delta functional business area.

BTS	Bureau of Transportation Statistics The Intermodal Surface Transportation Efficiency Act (ISTEA) of 1991 created BTS, a division of DOT, to administer data collection, analysis, and reporting and to ensure the most cost-effective use of transportation-monitoring resources.
Business area	A functional division of Delta A business area is a group of related functional sub-organizations of Delta.
CAA	Cargo Airline Association The CAA is an association for the all-cargo air carrier industry, and others in the air cargo marketplace that depend on these services. Located in Washington, D.C., the association represents the industry before regulatory bodies, the U.S. Congress and in the courts. (http://www.cargoair.com)
CAB	Civil Aeronautics Board The CAB was established by the Civil Aeronautics Act, which was signed into law by President Franklin D. Roosevelt in 1938. This law established the CAB as the U.S. federal agency charged with the power to regulate the economic aspect of air transportation. The CAB was charged with the general supervision and regulation of air carriers and their rates and routes.
Call Center	Delta Call Center As a cost cutting measure, Delta outsourced its telephone reservations operations to call centers, which were designed for receiving and sending a large volume of requests by telephone.
CAPPS II	Computer Assisted Passenger Pre-Screening program CAPPS II is a program developed by the U.S. government in 2001 that compares passengers' names, addresses, dates of birth, and other details against a database to determine the risk travelers posed to the aircraft.
CBP	U.S. Customs and Border Protection The CBP priority mission is keeping terrorists and their weapons from entering the United States.
CDTI	Cockpit Display of Traffic Information CDTI is used by pilots to aid navigation, esp. on approach to landing.
CIS	Computer Information Systems CIS was the Delta division that handled all information processing requirements of the company prior to the establishment of Worldspan and *Delta Technology*.
CISWG	Corporate Information Security Working Group The CISWG is a U.S. organization with members from the corporate, trade association, and academic arenas. CISWG works to develop a private-sector approach to securing U.S. information and infrastructure.

CM	Crisis Management Year 2000 CM was a coordinated effort among Delta sub-organizations for management in case of *Y2K* failure. For each sub-organization, a detailed Year 2000 CM Support Plan was developed that included requirements, procedures, and staffing (Delta archive, *Y2K* CM Delta Divisions.doc).
CM	Configuration Management CM is a system for managing large software development projects. A CM system automatically documents all components used to build executable programs. The system can recreate each build as well as recreate earlier environments in order to maintain previous versions of a product. It can also be used to prevent unauthorized access to files or to alert appropriate users when a file has been altered.
CMS	Conversational Monitor System CMS is software that provides interactive communication for IBM's Virtual Machine (VM) operating system. It allows a user or programmer to launch an application from a terminal and interactively work with it. The CMS counterpart in Multiple Virtual Storage (MVS) was Time Sharing Option (TSO). MVS, no longer supported by IBM, was the most commonly used operating system on the System/370 and System/390 IBM mainframe computers.
Code-sharing	Sharing airline codes—an arrangement whereby seats on one aircraft can be sold by two airlines. Under code-share agreements, Delta purchases seats on a foreign air carrier that are resold as Delta seats. These agreements are referred to as "Code-sharing" since seats on one aircraft were being sold by two airlines, with each carrier placing its own two-letter airline "code" (e.g., "DL") on the flight in the airline schedules and computer systems used by travel agents.
Connection carriers	Airline companies with whom Delta connects in order to provide passengers with service beyond a hub to a desired final destination. See Delta connection carriers.
COTS	Commercial Off The Shelf COTS refers to hardware or software acquired from sources external to Delta. Client/server and mainframe hardware platforms, operating systems, third party products, development tools, middleware products, database systems, applications software, and network components and protocols all fit into this category.
CP	Central Processor See CPU – Central Processing Unit.
CPDLC	Controller-Pilot Datalink Communications A CPDLC is an avionics system planned by FAA that links ground control to aircraft at enroute control centers (http://www.flttechonline.com).
CPU	Central Processing Unit The CPU (aka processor or microprocessor) is the brain of a computer—the central unit that performs the instructions of a computer's programs.

CRAF	Civil Reserve Air Fleet The CRAF program is a cooperative arrangement between U.S. military and commercial airlines, whereby commercial airlines supplement military resources to benefit national security.
Criticality	The value of an asset relative to operations During the Year 2000 Program, systems were assessed as to their "criticality," or importance to Delta and its operations.
CRM	Customer Relationship Management A collection of marketing and customer service processes meant to discover, retain, and grow customer value to the airline.
CRS	Computer Reservations System A CRS is a remote processing system for reserving aircraft seats electronically, and is used primarily by travel agents to book airline, hotel and car rental reservations and to issue airline tickets. Several airlines own and market such systems. The Global Distribution System (GDS) at Delta is an example. Other examples of CRS systems are Sabre, Apollo, Amadeus, and Worldspan.
CTL	Core Team Lead A CTL was a position within the Delta Year 2000 Program. The position had membership on the core team along with representing the team on a particular sub-project within the Year 2000 Program.
CTO	City Ticket Office Delta maintains a number of CTOs for facilitating customer transactions in other locations besides airports.
CTS	Common Test System A common set of data types in the Common Language Runtime environment of Microsoft's .NET platform.
Customs	An authority in a country that is responsible for enforcing the regulations related to import and export of animals and goods, and collecting tariffs. See U.S. Customs.
CWA	Communications Workers of America CWA is the largest communications and media union in the U.S., representing over 700,000 men and women in both private and public sectors. CWA members are employed in telecommunications, broadcasting, cable TV, journalism, publishing, electronics and general manufacturing, as well as airline customer service, government service, health care, education, and other fields (http://www.cwa-union.org/).
Data	Information based on fact Data is a collection of information that is used for analysis or for reasoning or making a decision.

Data mining	Data mining is a process of extracting and refining valuable information from a body of electronic data. Data mining in the analysis of the Year 2000 Program archive was challenging for this dissertation because of the inconsistency of formats and information design among the archive documents.
DBA	Database Administrator DBAs are responsible for the operation and administration of Database Management Systems (DBMS), and the creation of physical database designs and performance tuning (Delta archive, 1998, Mar 13, *Y2K* Engineering SOW.doc). .
DCI	Delta Connection, Inc DCI is a partnership arrangement established in 1984 that linked local "feeder" airlines serving mid-size population areas to Delta nodes.
Delta connection carriers	Connection carriers are airline companies with whom Delta connects in order to provide passengers with service beyond a hub to a desired final destination. Chautauqua, Comair, Freedom Airlines, Shuttle America, SkyWest, and ASA were Delta connection carriers, and were described as "high criticality suppliers / partners" because of their impact on Delta's passenger service and revenue.
DHS	U. S. Department of Homeland Security The DHS, a cabinet-level agency of the U.S. government, was established in 2002 to protect against and respond to threats and hazards to the nation, especially from terrorist attacks.
DLX	Delta Express DLX, a low fare carrier, was a business unit of Delta that operated short- to medium-haul flights into and out of Florida.
DMSS	Data Management Support System DMSS software supports functional capabilities of a project, providing monitoring, maintenance and control of information.
DNS	Delta Nervous System DNS is the IT infrastructure system implemented as a part of Delta's IT transformation between 1997 and 2003. This integrated network links all of Delta's communication and information functions, and allows all business areas of Delta to share real-time information with customers and / or employees.
DOT	U. S. Department of Transportation An act of Congress on October 15, 1966 established the U.S. DOT as a cabinet-level agency of the U.S. government. The mission of the Department is to "serve the United States by ensuring a fast, safe, efficient, accessible and convenient transportation system that meets our vital national interests and enhances the quality of life of the American people, today and into the future" (http://www.dot.gov).

DSO — Data Source Object

A DSO is a Microsoft *ActiveX object* embedded within a Web page. It employs a process called data binding, whereby the *ActiveX control* communicates directly with another Web page, or with an external XML data source. A DSO exploit is a form of spyware that takes advantage of data binding to gain access to the hard drive of a computer that is connected to the Internet.

DT — Delta Technology

DT is the subsidiary business unit of Delta that provides information technology development and support exclusively for the airline.

EAS — Essential Air Service

When the federal government deregulated the airlines in 1978, the EAS program eased concerns that smaller communities would be stranded without air service. The program guaranteed that towns that had air service as of October 1978—provided they were farther than 70 miles from a larger airport—would be eligible for subsidy in order to keep that service in place.

EC — Executive Council

The EC is the top tier of Delta decision makers.

ECD — Estimated Completion Date

Assignment of an ECD was important for the management, esp. the planning and status reporting, of projects in the Delta Year 2000 Program.

EPIC — Electronic Privacy Information Center

EPIC, a nonprofit public interest research center in Washington, D.C., was established in 1994 to focus public attention on civil liberties issues especially the protection of privacy (http://www.epic.org/).

ERISA — Employee Retirement Income Security Act: signed into law by President Ford in 1974.

Delta sponsors qualified and defined benefit pension plans for eligible employees and retirees. The company's funding obligations under these plans are governed by ERISA.

E-SIGN — Electronic Signatures in Global and National Commerce Act: signed into law by President Clinton in 2000.

E-SIGN facilitates the use of electronic records and signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically (http://www.ftc.gov/os/2001/06/esign7.htm).

FAA — Federal Aviation Administration

The FAA, created in 1958 as an agency of the U.S. government, is responsible for the safety of civil aviation. The agency became a part of the DOT in 1967.

FAR — Federal Aviation Regulation

FARs are rules prescribed by the FAA to promote safe aviation, designed to protect pilots, passengers and the general public from unnecessary risk. The FARs—part of Title 14 of the Code of Federal Regulations—address "every conceivable aspect of aviation safety" (Hamilton, 2001, p. 4).

Flight superintendent	A title and a role in air traffic control. A Flight Superintendent is an employee assigned to dispatch, clear, and control flights operated by Delta and its subsidiary organizations. See PAF-CA.
FPS	Flight Planning System The FPS is a program that automatically transfers flight plans & databases to the aircraft's data transfer module (DTM).
FSF	Flight Safety Foundation FSF is an international non-profit organization where air carriers, manufacturers, suppliers, maintenance organizations, aviation regulatory agencies, and flight crewmembers share information, ideas and best practices for safety (http://www.flightsafety.org/home.html).
GA	General Aviation General aviation is defined as all aviation other than military and commercial airlines.
GAAP	Generally Accepted Accounting Principles In the U.S, GAAP are accounting rules used to prepare, present, and report financial statements for publicly-traded companies and many privately-held companies. The government does not directly set accounting standards, in the belief that the private sector has better knowledge and resources. US GAAP is not written in law, although the SEC requires that it be followed in financial reporting by publicly-traded companies.
GAMA	General Aviation Manufacturers Association Since its inception in 1970, the General Aviation Manufacturers Association (GAMA) has strived to be a reliable source of information among the aviation trade press and the national media regarding general aviation (GA). See GA. (http://www.gama.aero).
GARA	General Aviation Revitalization Act: signed into law by President Clinton in 1994. GARA was designed to protect manufacturers of smaller, private aircraft (less than 20 seats) from liability for accidents involving older airplanes and/or parts. GARA bars lawsuits against the manufacturer of an aircraft or component part in service more than 18 years. GARA does not apply if the aircraft was engaged in scheduled passenger-carrying or air medical services operations at the time of an accident (http://www.house.gov/transportation/aviation/).
GDS	Global Distribution System See CRS.
GEMA	Georgia Emergency Management Agency The Georgia Emergency Management Agency (GEMA) operates under the authority of the Emergency Management Act of 1981. Virtually all GEMA employees are on 24-hour call to assist local authorities in responding to emergencies. In addition, they staff the State Operations Center (SOC) when a disaster or emergency threatens, as well as prior to and during large scale events. (http://www2.state.ga.us/GEMA/).

GID	Gate Information Display GIDs are plasma screens that Delta installed at airports across the U.S. in 2002. The screens are updated continuously with real time flight status, weather, seating configuration, standby and upgrade lists, boarding status, onboard service, cancellations, and gate changes.
GLBA	Gramm-Leach-Bliley Act: signed into law by President Clinton in 1999. GLBA, also known as the Financial Services Modernization Act of 1999, allows banks to engage in a wide range of financial services, and provides privacy protections against the sale of private financial information. Additionally, the GLBA codifies protections against pretexting, the practice of obtaining personal information through false pretenses (http://www.epic.org/privacy/glba/).
GO facilities	Ground Operations A GO crew tags, loads and unloads baggage, operates GSE, coordinates the service and surface movement of arriving and departing aircraft at an airport.
GSE	Ground Service Equipment GSE refers to airport equipment such as baggage tugs and jetways.
HIPAA	Health Insurance Portability and Accountability Act: signed into law by President Clinton in 1996. The HIPAA Act amended the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to simplify the administration of health insurance, and for other purposes. The law requires the adoption of security and privacy standards in order to protect personal health information. HIPAA had been called "*Y2K* on steroids" (http://www.hhs.gov/news/press/2002pres/hipaa.html).
Hub and spoke	A network design adopted by major air carriers. In a hub and spoke routing design, planes bring passengers to a "hub" airport where they connect to other flights enroute to other destinations. The spokes are the routes that planes take out of the hub airport. Delta was an early pioneer in the use of the hub and spoke concept in 1955.
IAPA	International Airline Passenger Association The IAPA was established in 1960 to represent the interests of frequent air travelers by providing group discounts on items such as hotel accommodation, car rental and insurance, in addition to protecting and promoting their rights as airline passengers. The organization has over 400,000 members in over 200 countries (http://www.iapa.com).
IATA	International Air Transport Association IATA is the global trade organization for air transportation, and plays an important role in harmonizing technical standards for civil aviation worldwide. Its members comprise 265 airlines—the world's leading passenger and cargo airlines—representing 94% of international scheduled air traffic. IATA members, as scheduled and non-scheduled airlines, operate commercial air services from more than 140 nations (http://www.iata.org).

ICAO — International Civil Aviation Organization

ICAO, a specialized agency of the U.N., works toward safe, secure, and sustainable development of civil aviation through cooperation among its member nation-states. ICAO establishes international standards and recommended practices and procedures in the technical fields of aviation, which includes promoting security and the safe transport of dangerous goods (http://www.icao.int/).

ICS — Integrated Customer Service

ICS was an internal Delta initiative—a cross-divisional project focused on improving customer service.

IFALPA — International Federation of Air line Pilot Associations

IFALPA is made up of around 100 national member pilot associations—approximately 120,000 airline pilot members out of the estimated 150,000 active pilots (http://www.ifalpa.org).

IFATCA — International Federation of Air Traffic Controllers Associations

IFATCA is a professional organization representing around 40,000 air traffic controllers in over 100 countries (http://www.ifatca.org).

IFBP — In-flight Broadcast Procedure

A form of air traffic control whereby pilots move their aircraft to new altitudes based on the locations of other planes nearby.

IFEO — International Flight Engineers Organization

The International Flight Engineers Organization (IFEO) has merged with the International Federation of Air Line Pilots' Associations (IFALPA) (http://www.ifalpa.org).

IFS — In-Flight Service

IFS is the Delta division that includes flight attendants and onboard services.

IG — Implementation Group

An IG was a logical group of COTS products formed [in order] to plan, schedule, renovate, test, and implement *Y2K* compliant versions. Each IG had an IG Owner (See Roles & Responsibilities description in presentation handout) … (Delta archive, Workshop Presentation.ppt).

INS — U.S Immigration and Naturalization Service (now USCIS)

On March 1, 2003, the service and benefit functions of the U.S. Immigration and Naturalization Service (INS) transitioned into the Department of Homeland Security (DHS) to become the U.S. Citizenship and Immigration Services (USCIS). See USCIS**.**

ISAC — Information Sharing and Analysis Center

ISACs are organizations that represent a cooperative effort between the federal government and private organizations to share information by industry sector in support of increasing information security (e.g., see the IT-ISAC website: https://www.it-isac.org/).

IT infrastructure	Common IT services shared by multiple systems IT infrastructure includes computer-based hardware, software, network components, etc.
ITO / BPO	IT Outsourcing / Business Process Outsourcing Outsourced information technology [IT] services, as well as other business processing functions that are IT-enabled, are increasingly going offshore (Westby, 2007).
JAA	European Joint Aviation Authorities The JAA is an organization of the European Civil Aviation Conference (ECAC) representing the civil aviation regulatory authorities of European States who have agreed to co-operate in developing and implementing common safety regulatory standards and procedures for aviation.
LCC	Lower Cost Carriers LCCs are airline organizations, e.g., jetBlue, Southwest, Frontier, and AirTran, that began after deregulation in 1978 as competitors to the network carriers.
LOC	Lines of Code The progress of eliminating the *Y2K* bug from Delta systems was tracked by *Delta Technology* portfolio groups based on the number of LOCs that had been examined.
McKinsey	McKinsey & Company McKinsey is a privately owned management consulting firm that focuses on solving issues of concern to senior management in large corporations and organizations.
Middleware	Software that provides interoperability with mainframe transaction systems. The use of middleware is a way to access data on legacy mainframe systems for a client/server environment, allowing most of the existing applications and infrastructure to remain in place (e.g., IBM's MQSeries middleware).
MVS	Multiple Virtual Storage MVS is an IBM proprietary operating system, designed for large scale systems. During the Year 2000 Program, Delta set up a test environment for applications that depended on MVS.
NACA	National Advisory Committee for Aeronautics NACA was established in 1915 by the U.S. Congress as an organization dedicated to the science of flight. NACA was operational until 1958, when the National Aeronautics and Space Act of 1958 created NASA from NACA (http://history.nasa.gov/naca/index.html).
NACO	National Aeronautical Charting Office NACO, a department of the FAA, publishes and distributes aeronautical charts and flight information publications (http://www.naco.faa.gov).
NAS	National Airspace System NAS refers to the organization of entities and technologies relating to maintenance of flight safety in U.S. air space.

NASA	National Aeronautics and Space Administration See NACA.
NMB	National Mediation Board The NMB was established by the 1934 amendments to the Railway Labor Act of 1926. It is an independent agency that attempts to facilitate harmonious labor-management relations within two of the nation's key transportation modes—railroads and airlines.
Network airlines (carriers)	Network airlines are major airlines, the hub-and-spoke operators. Network airlines included American, TWA, Delta, United, Northwest, Continental, US Airways, America West, and Alaska.
Non-IT	Equipment [containing embedded computer chips] used by Delta in distribution, production, services, or general office environments. Some examples include, but are not limited to planes, parts, tools, tugs, forklifts, cars, TVs, LCDs, copiers, postage meters, etc. (Delta archive, Definiti.doc).
NSCIATS	National Safety Council's International Air Transport Section The National Safety Council (NSC) is a nonprofit NGO international public service organization. The IATS membership is comprised of airlines, airport operators, and related organizations; the scope is operations such as ramp operations, fuel and cabin servicing, GO, and facilities maintenance (http://www.nsc.org/mem/indus/sect/intlair/intlair.htm).
NWS	National Weather Service Formerly the Weather Bureau, renamed NWS in 1967. NWS is a division of the National Oceanic and Atmospheric Administration (http://www.nws.noaa.gov).
OAEP	Office of Aviation Enforcement and Proceedings The OAEP is a division of the DOT, under the office of the General Council. The office provides investigative support, public counsel, legal prosecution for various cases regarding compliance with DOT aviation regulations.
OC	Operating Council A committee of the Delta Year 2000 Program comprised of Portfolio Leads and Portfolio Directors. This group met periodically to deal with technical issues related to IT systems.
OCC	Operations Control Center The OCC is a division in Delta's *Operations* business area that monitors flight progress. Displays show all of the Delta flights wherever they are, all the way to the ground.
OES	Open Enterprise Server OES is an open-source server by Novell, designed for delivering business-area applications in networked environments. It includes NetWare, the long-standing leader in networking services, and SUSE Linux Enterprise Server, an open source product (http://www.novell.com/products/openenterpriseserver/).

OSHA	Occupational Safety and Health Administration Congress created OSHA under the Occupational Safety and Health Act, signed by President Nixon in 1970. OSHA's mission is to prevent work-related injuries, illnesses, and deaths.
PAF-CA	Professional Airline Flight-Control Association PAF-CA is a collective bargaining unit representing aircraft dispatchers and operational control employees at Delta, ASA, and United.
PD	Point Director The Point Directors were Year 2000 team leaders in *Delta Technology* that reported to the Portfolio VPs (*Airport Customer Service*, *Operations*, *Business Support*, and *Revenue*).
PD	Portfolio Director A PD in a *Delta Technology* group spent some percentage less than 100% of their work effort—maybe 30%—on *Y2K*.
PDN	Personnel Department Number A PDN is a number assigned to a Delta department for accounting purposes.
PL	Portfolio Lead A PL was the *Y2K* point person in a *Delta Technology* group who was dedicated 100% to *Y2K*.
PMO	Program Management Office The PMO was a department in the Delta organization that was created in order to coordinate the activities of the enterprise-wide Year 2000 Program.
PMSR	Program Management Status Review The PMSR was a weekly status update designed to inform the Program Manager and other key people, internal and external to the program, of Delta Year2000 Program status.
Portfolio	A division of labor in the *Delta Technology* organization Activities within the four application portfolios included development and maintenance of systems that supported the activities of the four corresponding business areas in Delta.
PPP	Public Private Partnership PPP is a system in which a government service or private business venture is funded and operated through a partnership of government and one or more private sector companies (http://en.wikipedia.org/).
PVP	Portfolio Vice President The PVP was a top-level administrator in the *Delta Technology* organization who was responsible for the IT systems in one of the business areas in the Delta organization (*Airport Customer Service*, *Operations*, *Business Support*, or *Revenue*).

RLA	Railway Labor Act: signed into law by President Roosevelt in 1926 and amended in 1936 to apply to the airline industry. The RLA governs labor relations in the railway and airline industries in the U.S. The Act sought to substitute bargaining, arbitration and mediation for strikes as a means of resolving labor disputes. Delta is a common carrier by air as defined in 45 U.S.C. § 181, of the Railway Labor Act.
RTCA	Radio Technical Commission for Aeronautics A private, non-profit, global corporation that develops consensus-based recommendations regarding communications, navigation, surveillance, and air traffic management (CNS / ATM). Organized in 1935 as the Radio Technical Commission for Aeronautics, RCTA includes 335 government, industry, and academic organizations. Domestic membership includes, among others, FAA, ALPA, ATA, AOPA, ARINC, Avwrite, Boeing, DOD, GARMIN, Rockwell, Stanford Univ, Lockheed Martin, MIT Lincoln Lab, MITRE / CAASD, Harris Corp, NASA, NBAA, and Raytheon (http://www.rtca.org).
SEC	Securities and Exchange Commission The mission of the U.S. SEC is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation.
SIMS	Simulator Systems - flight training equipment Delta incorporates SIMS into the routines involved with pilot certification on particular aircraft.
SkyTeam	A global airline alliance SkyTeam members are airlines that maintain international code-share agreements with Delta. These arrangements provide customers access to worldwide destinations, flights, and services.
SME	Subject Matter Experts SMEs are Delta employees who have working knowledge of particular subject matter applicable to Delta operations and IT systems.
SPA	SkyTeam Pilots Association The SPA comprises pilots from nine global SkyTeam member carriers. The carriers are Delta, Northwest, AeroMexico, Alitalia, CSA Czech, KLM, Air France, Korean Air, and Continental.
SOA	Service-oriented architectures SOAs “treat applications as reusable services,” thereby reducing redundancy in related applications. This concept considers mission-critical legacy software applications as too valuable to “convert” to a new platform, therefore enables greater efficiency and flexibility by identifying common services to which they can link (Knorr, 2004).
SOA	Sarbanes-Oxley Act: signed into law by President Bush in 2002 SOA, commonly called “SOX” or “SarbOx,” covers establishing a public company accounting oversight board, auditor independence, corporate responsibility, and enhanced financial disclosure. Considered one of the most significant changes to the U.S. securities laws since the New Deal in the 1930s, it was designed to review the dated legislative audit requirements. The Act gave additional powers and responsibilities to the SEC.

STAR	Standard Terminal Arrival Route STAR charts are used by pilots in aircraft cockpits to assist in navigation.
TCAS	Traffic alert and Collision Avoidance System TCAS is an instrument integrated into other systems in an aircraft cockpit. It consists of hardware and software that together provide a set of electronic eyes so the pilot can "see" the traffic situation near the aircraft (http://www.mitrecaasd.org/work/project_details.cfm?item_id=153).
Threat	A threat to the reliable operation of a computer-based system A threat exists when there is an agent that places a system vulnerability at risk of exploitation. This dissertation limits focus to the human agent, apart from natural causes (e.g., weather related damage).
TIA	Travel Industry Association of America TIA is a non-profit trade association that represents the common interests and concerns of the U.S. travel industry (TIA website).
Tier I, II, III	A description assigned to an airport The tier description of an airport is based on its features for accommodating types of aircraft, and air traffic services.
TCC	Technology Control Center TCC is a facility at Delta's headquarters campus for viewing and interacting with its IT network. Employees at the TCC view and monitor real-time activity and deal with issues in Delta IT systems world-wide.
TOC	Technical Operations Center The TOC is Delta's maintenance operations facility in Atlanta, located at Hartsfield airport. TOC is also called the Jetbase.
TPF	Transaction Processing Facility TPF is the software engine behind airline, hotel, and rental car reservations systems. It is a real-time mainframe *operating system* released by IBM around 1976, and retooled in 2004 for Linux. TPF is particularly well suited for organizations dealing in very high I/O message switching and large global networks. Users include British Airways (reservations), VISA International (authorizations), Holiday Inn, and Delta. TPF was traditionally an IBM370/Assembler environment although release 4.1 contained C. It was common for TPF sites to use IBM's MVS and VM operating systems for off-line processing (Lohr, 2004).
TQ	TransQuest *Delta Technology* was formerly called *TransQuest*. *Delta Technology*, a wholly owned subsidiary organization of Delta is charged with developing and maintaining IT systems for the airline.
TRW / BDM	TRW, Inc. / BDM International, Inc. In 1997, TRW purchased BDM, an IT consulting company, especially for its integrated supply chain management and enterprise management businesses. TRW's business mix was 60% automotive; the remaining related to defense and space (http://www.trw.com).

TSE	Test System Engineer A TSE was a role during Delta's Year 2000 Program. These employees provided assistance to the business area teams by evaluating the remediated software in a test environment before it was placed in production.
TWU	Transport Workers Union of America TWU, a trade union representing workers in mass transportation, airline, railroad, utility, university, municipalities, service and allied industries, is affiliated with the American Federation of Labor and Congress of Industrial Organizations (AFL-CIO) and the worldwide International Transport Workers Federation (ITF). The organization was founded in 1934 as an industrial union dedicated to the idea of trust and equality for all workers.
USAIG	United States Aircraft Insurance Group USAIG is a group of insurers that collectively functions as a global aviation insurance market. The group participates in insurance programs for 80 % of U.S. airlines and is the lead insurer for Delta.
UEB	Universal Enterprise Build The UEB was a "design stack" for the standardization of desktop units across the Delta enterprise.
USA Patriot Act	The USA Patriot Act: signed into law by President Bush in 2001. The Patriot Act requires appropriate tools to intercept and obstruct terrorism, and has far-reaching consequences for computer privacy and information security. Enacted a month after the Sept. 11, 2001, terrorist attacks, the Patriot Act became a target of criticism for giving police broad powers and allegedly curbing civil liberties in the process.
USCIS	U.S. Citizenship and Immigration Services Formerly known as the INS, USCIS is responsible for the administration of immigration and naturalization adjudication functions and establishing immigration services policies and priorities.
U.S. Customs	United States Customs Service (Now CBP) On March 1, 2003, the service and benefit functions of the U.S. Customs Service transitioned into the Department of Homeland Security (DHS) to become the U.S. Customs and Border Protection (CBP). See CBP**.**
VM	Virtual Machine (also known as CMS) VM is a mainframe-based system operated by Worldspan and used by Delta, *Delta Technology*, and Worldspan. Delta established a Year 2000 VM testing environment, and coordinated construction and implementation of platforms with Worldspan.
VPP	The Voluntary Protection Programs Cooperative programs of OSHA "promote effective worksite-based safety and health." In the VPP, an organization's management, labor, and OSHA establish cooperative relationships at qualified workplaces that have implemented a comprehensive safety and health management system. Approval into VPP recognizes workplaces with exemplary safety and health programs and exempts them from routine OSHA inspections (http://www.osha.gov/dcsp/vpp/).

Vulnerability	A weakness in a computer-based system A vulnerability creates a risk that a system will malfunction, caused by misuse or other system condition.
WBS	Work-Breakdown-Structure WBS was a part of the Year 2000 Program methodology whereby a project was implemented via a delegated structure of responsibilities.
WGE	Workgroup Engineering WGE is the division of *Delta Technology* that is responsible for configuration and maintenance of end-user computing products.
Workgroup	A designation related to local area networks In *Delta Technology*, a workgroup refers to an end-user: a workgroup product is a computer—desktop or laptop, or NT server for files and printing.
WSP	Worldspan Developed as an outsourced reservations function of Delta, a consortium of airline companies owns and operates Worldspan (WSP). WSP provides comprehensive electronic data services linking approximately 800 travel suppliers around the world to a global customer base. Delta sold its 38% interest in 2003 (http://www.worldspan.com/).
Y2K	Year 2000 The acronym *Y2K* is associated with the computer programming practice that created a worldwide crisis. When world clocks moved from 1999 to 2000, computer-based systems that had not been replaced or their programming code adequately repaired produced erroneous calculations and either malfunctioned or ceased to function.
Y2K solution	Changes to IT systems that eliminated the *Y2K* code *Y2K solution* is the dependent variable in the research model of this dissertation. A *Y2K solution* is defined as changes to *software systems* in a functional business area of Delta over the period 1997-2003.
Year 2000 Act	The Year 2000 Information Readiness Disclosure Act: signed into law by President Clinton in 1998. Designed to encourage disclosure, the Year 2000 Act provided makers of Year 2000 Statements with immunity from liability in civil actions based on allegedly false, inaccurate, or misleading Year 2000 Statements. Statements were defined as communications concerning the Year 2000 readiness of products or services made by one party to another party from July 14, 1998 through July 14, 2001.

TIMELINE

This section presents an overview of Delta's history in order to introduce the reader to the case study context. The essential foundation for this dissertation is based on the concept of institutionalized environment, and therefore, strongly relates to the history of Delta, its culture and its sectoral institutions. Entries in this timeline represent significant events or milestones that indicate Delta's continuous growth, increasing complexity, military and union connections, and its background in computer technology. Also notable is Delta's consistency of achievements in flight safety. Milestones in Delta's history that relate to information technologies are in boldface type.

1929	Delta operates its first passenger flights.
1942	Delta contributes to the war effort, modifying 1,000+ aircraft, over-hauling engines/instruments, and training Army pilots and mechanics.
1945	Official corporate name becomes Delta Air Lines, Inc. Delta receives the National Safety Council Award for over 300 million passenger miles and 10 years of flight without a passenger or crew fatality. C. E. Woolman is President and General Manager.
1946	Delta starts regularly scheduled cargo service. The one-millionth passenger boards.
1947	Delta receives the National Safety Award for more than one-half billion passenger-miles without a fatality.
1948	As the first U.S. interchange service, TWA crews fly Delta planes from Cincinnati to Detroit; Delta crews fly TWA planes south to Atlanta, Miami, and Dallas.
1953	Delta acquires its first international routes—to the Caribbean and Caracas—via merger with Chicago and Southern Air Lines. Delta-C&S is the name of the merged airline for the next two years.
1955	Delta pioneers the use of the hub and spoke system in the U.S.

1956 Radar is installed in the noses of all Delta aircraft.

1957 Delta stock begins trading on the New York Stock Exchange.

1959 Delta is the first airline to launch jet service.
The red, white, and blue triangle "widget" becomes Delta's logo.

1961 Delta receives the National Safety Award for flying over 11 billion passenger miles without a fatality.
Charles Gravitt joins Delta as a communications specialist (Gravitt later plays a major role in Delta's Year 2000 Program.).

1962 **Delta activates the SABRE system for electronic reservations.**

1964 **IBM develops and installs the Deltamatic reservation system on Delta's IBM 7074 computers.**

1966 **Delta begins computer training in-house.**
Delta founder and CEO C.E. Woolman dies.
The crop-dusting division ceases operations.
Charles H. Dolson becomes Delta's second CEO.

1970 Delta has an all-jet passenger airplane fleet.
Apollo 13 moon landing mission is aborted, but returns its crew safely to Earth.

1971 W.T. Beebe becomes Chairman and CEO.
Delta Dash (cargo service for small packages) begins operations.

1972 Northeast Airlines merges with Delta.

1974 Gravitt becomes General Manager, Computer Information Systems (CIS).

1975 *Delta Air Express* begins operations, making Delta the first airline to offer its own "express delivery guaranteed" cargo service.

1978 The Airline Deregulation Act passes.
Delta begins flying transatlantic service: Atlanta to London.
David C. Garrett becomes CEO.

1979 Delta boards one million passengers in one city in one month—first airline in the world to experience this level of customer activity (Atlanta, in August).

1980 **In the early 1980s, Delta IT personnel develop DATAS II computer reservations system (CRS).**

1981 Delta launches Frequent Flyer Program (changed to *SkyMiles* in 1995).
Delta forms Epsilon Trading Corp., a computerized marketing subsidiary, to coordinate and sell more passenger seats on all Delta flights.

1982 After Delta reports financial losses, its employees raise $30 million in payroll deductions to purchase the first Boeing 767, named "The Spirit of Delta."

1984 Delta begins its *Delta Connections* program, designed to strengthen relationships with regional airline partners.
Delta offers the U.S. first public air-to-ground telephone system with *Airfone*, on the Lockheed L-1011.

1985 **Delta's data communications network comprises over 400 privately leased lines that serve over 3,000 locations.**

1987 Via merger with Western Airlines, Delta becomes the fourth largest U.S. carrier and fifth largest world carrier.
Delta offers its *DeltaStar*® PC-based CRS to independent travel agencies (DATAS II).
Ronald W. Allen becomes Chairman and CEO.

1990 Delta and 23 civilian airlines participate in the Civil Reserve Air Fleet (CRAF) during Desert Storm/Desert Shield from 1990-1991, carrying passengers and military cargo.
Delta, Northwest Airlines and TWA combine computer-based reservations systems (CRS) to form *Worldspan Travel Information Services*.

1991 Delta purchases Pan Am's transatlantic routes and the Pan Am Shuttle—the largest acquisition of flights in airline history.
Delta becomes a global carrier.
Delta signs with DEC to develop its Technical Operations Publishing System (TOPS) for aircraft maintenance schedules and documentation—the first online maintenance information system in the airline industry.

1993 Computerworld (de Jaeger, 1993) publishes Peter de Jager's article, entitled "Doomsday 2000." The article describes the "catastrophe" that would ensue if mainframes could not process "2000" by the year 2000.
***Worldspan* enters the airline technology services business.**

1994 Because of massive economic losses, Delta CEO Allen announces an aggressive cost-cutting program—Leadership 7.5.
Ray Valeika, formerly with Continental, joins Delta as VP-Technical Ops.
***Worldspan* introduces the first full Microsoft® Windows®-compatible workstation environment for travel agencies.**

1995 In partnership with AT&T, **Delta outsources the balance of its IT services to a new subsidiary organization called *TransQuest Information Solutions***. William Belew, CIO at W.R. Grace & Co., becomes President and CEO of the new company. Delta's IT personnel become *TransQuest* employees.
Delta names James McCullough Director of IT, providing oversight for a **new internal IT department—about 100 IT staff who remained at Delta to serve as technology liaison among Delta, *TransQuest*, and *Worldspan*.**
Year 2000 activities begin at *Worldspan* in July 1995.
The 1996 Centennial Olympic Games names Delta as official airline; J.D. Power & Associates honors Delta as the best in long and short haul flights among major carriers.
Delta returns to profitability in the fourth quarter, fiscal year 1995.
Year 2000 activities begin at *TransQuest* in December 1995.

1996 Delta starts a low-fare airline, *Delta Express*.
Delta powers up its Operation Control Center (OCC), a new computerized flight management facility.
Delta's website, *SkyLinks*, enables customers to make reservations and purchase tickets online.
***TransQuest* partnership is dissolved;** *TransQuest* becomes a wholly owned Delta subsidiary supporting Delta's functional business areas exclusively.
Delta begins formally addressing the *Y2K* problem in June of 1996, and launches a structured program for eliminating the *Y2K* vulnerability in its systems and equipment in October.
***TransQuest* begins inventory of IT systems in Dec 1996.**

1997 Delta is the first airline to board over 100 million passengers in a year.
Belew resigns from *TransQuest*; Paul Matson, Sr. VP-Corporate Strategy and Planning is interim replacement.
Mac Armstrong joins Delta as Exec VP-Operations in June.
Delta announces the Year 2000 Program via internal publications: July 30 issue of *Heads Up*, and Aug 1 issue of Delta *NewsDigest*.
Leo F. Mullin comes on board as President and CEO on August 14.
Charlie Feld is named interim Delta CIO, and *TransQuest* CEO.
Tom Roerk, CFO since 1987, resigns in November.
TransQuest* is renamed *Delta Technology, Inc.

1998 Delta and SwissCargo create the first international cargo alliance.
ATA *Y2K* industry initiative begins in January.
Delta Year 2000 Program reorganizes in March. Matson leads the IT Board. Feld becomes executive sponsor "responsible for the successful completion of all aspects of the Year 2000 program"; Walter Taylor, *Delta Technology* VP-Airline Operations Systems, is named Year 2000 Program director in April. Gravitt is Year 2000 managing director.
Benjamin R. DeCosta is named aviation general manager for Hartsfield International Airport in June.
Year 2000 Desktop Strategy Project kicks off at Delta in September.

1999 Air Transport World magazine names Delta "Global Airline of the Year" for 1998.
Aviation Week and Space Technology magazine names Delta 1999's "Best Managed Major Airline."

2000 **Delta announces *Y2K* success.**
Flight attendant scheduling system malfunctions, along with around 40 non-critical systems.
Bob DeRodes becomes Delta CIO.
Delta carries 120 million passengers.
Partnering with AeroMexico, Air France and Korean Air, Delta launches the *SkyTeam* global alliance.
Delta acquires *Atlantic Southeast Airlines* and *Comair*, two regional *Delta Connection* carriers, as wholly owned subsidiaries.
***Delta.com* web site goes live.**
***Delta Technology* receives the Computerworld Smithsonian Award for the *Delta Technology* Customer Care System.**
50,000 personal computers are distributed to employees, to increase familiarity with IT.
Delta signs in September to run its pricing and reservations operations on a farm of Hewlett-Packard Unix servers with software from ITA Software.

2001 U.S. airspace is closed for two days after terrorist attacks on Sept. 11th.
Delta posts its first financial loss in six years.
***Delta.com* surpassed the $1 billion mark for 2001 ticket revenue on Nov 13.**

2002 Curtis Robb becomes *Delta Technology* CEO, Delta CIO.
New IT systems are installed—kiosks at check-in, expanded gate information systems, and virtual check-in on *delta.com*.
Flight attendants reject AFA representation; … "to remain union-free by overwhelming majority" (Cason, 2002, p. 12).
International Air Transport Association (IATA) ranked Hartsfield number one in overall passenger satisfaction for large hub airports in 2002.
Profit Improvement Initiative begins (savings goal of $5 billion).

2003 Delta launches *Song*®, a low-cost subsidiary airline, replacing *Delta Express*.
Delta implements the largest domestic code-share alliance with Continental and Northwest.
SkyTeam is the world's largest leading airline alliance.
Massive cutback of flights in March because of the war in Iraq. Delta eliminates roughly 16,000 jobs (21 percent of its workforce compared to pre-Sept. 11 levels) by mid-2003.
Delta sells its interest in *Worldspan*.
Delta introduces a new model for passenger check-in: lobby redesign, expanded kiosk function, agents to assist in the ticket lobby, *Delta Direct* phone banks.
Delta is the first U.S. airline to offer prerecorded audio flight information at the gate. **New ramp technology is installed**, which is designed to improve fuel savings, load and unload times, and baggage transfer.
Delta establishes an Information Security department, headed by Spark Nowak as Chief Information Security Officer.
Mullin steps down as CEO at year-end. Board member and industry veteran Gerald Grinstein replaces Mullin as CEO.
100-year anniversary of the Wright Brothers' flight at Kitty Hawk, N.C.

2004 **Mullin resigns** as Chairman of the Board in April.
A "systems glitch" forced Delta to cancel about 40 flights and delay an unspecified number of departures on May 1 ("Delta stays mum on cause of IT glitch," 2004).
Comair IT systems crash on Christmas Day.

2005 Delta and its subsidiaries filed to reorganize under Chapter 11 in the U.S. Bankruptcy Court on Sept. 14.

SUMMARY

Computer-based information and communication technologies have become indispensable components of modern organizations. However, historical evidence shows that both a growing reliance on computer-based systems and their pervasive use have created new threats to organizational assets and infrastructure systems. Caused by the growing complexity and proliferation of these systems, their vulnerabilities have outpaced technical and non-technical means for making them reliable and adequately secure.[2] As an example, in the late 1990s organizations tackled an information security problem of unprecedented scale. A small detail written into the code of computer-based systems before the year 2000, often called the "*Y2K* bug," emerged to create a worldwide crisis. Different from most crises or other failures, the *Y2K* bug affected not just a few isolated organizations; a vast number of organizations required changes to systems during the same period, and their networked environments complicated the process. At best, the *Y2K* problem represented a potential interruption to the normal workflow of an organization. At worst, the problem jeopardized the reliability and the ultimate safety of critical infrastructure operations worldwide.

Because of the networks over which electronic information travels, a great deal of current discourse has identified environments as a source of information security problems. Further, among environmental sources, many of the security problems are non-technical—resulting from the lack of harmony in legal systems, and the cultural differences that complicate operations of global organizations, among other issues.

[2] "Non-technical means" include laws, policies, education, i.e., methods apart from hardware and software coding.

Historically, however, efforts to improve the security of computer-based systems have focused on technical system components, i.e., hardware and software. Researchers and practitioners now understand that non-technical issues are significant—equal to if not more important than technical issues, and that those at the environmental level are especially difficult to manage.

Very little empirical research exists in the non-technical-environmental area of information security. Therefore, helping to fill this gap, the purpose of this theoretically based dissertation was to understand ways in which institutionalized environments influence information security in large, complex organizations. The successful elimination of the *Y2K* vulnerability provided a model to study how organizations contend with problems affecting the security of electronically stored and transmitted information, and how context influences their solutions.[3] The investigation applied rival theories of organization from the sociological literature to analyze organization actions.

This dissertation presents a case study set around the Year 2000 Program at Delta Air Lines (Delta), a complex U.S.-based transportation organization. Employing a comparative-case method, the dissertation explained the variation in 1997-2003 compliance solutions among four business areas, as embedded cases.[4] Data for the investigation were the Delta Year 2000 Program archive, personal interviews with individuals related to the Delta Year 2000 Program, and secondary sources. Evidence

---

[3] A vulnerability is a *weakness in a computer-based information system.* A vulnerability creates a risk that a system will malfunction, caused by misuse or other system failure.

[4] For management purposes, Delta organized its IT systems as "portfolios" of systems. The portfolios of interest to this study were the software systems that corresponded to the four core business areas.

revealed characteristics of both the institutional and the rational-contingency models of organization.

The case highlights how analyzing institutionalized environments can broaden perceptions and increase understanding of information security, thus enhancing the possibility to engage new mechanisms for technological and organizational management. Case results showed that:

- A positive relationship among entities in the sectoral environment benefited the air transportation field in addressing the *Y2K* problem. In this cooperative setting, addressing common issues in one place helped a vast network of related organizations. Recognizing that all were stakeholders made it work.
- Business area decisions were influenced by the institutionalized environments of their respective fields.
- In the process of eliminating the *Y2K* bug from the Delta systems, new vulnerabilities were introduced. While tradeoffs are always required among security, functionality, and efficiency within the structures and IT systems of the present time, this negative effect might have been anticipated; but it was not.
- The Year 2000 Program team lacked awareness and consideration that the *Y2K* bug was an information security issue.
- The success of this complex, short-term project at Delta underscored the importance of leadership, understanding of IT, vision, motivation, IT skills, understanding of assets, and appropriate strategy.

The Delta case study contributes to the field of organization studies. Results also have implications for policymaking and for future research in the field of information security.

CHAPTER 1

HOUSTON, WE'VE HAD A PROBLEM

> Halfway to the moon, an explosion in the service module destroyed Apollo 13's oxygen and power equipment. … Jack Swigert's first report of a problem is buried under another exchange on Flight's loop, but you can faintly hear Lovell's famous "Houston, we've had a problem" a few seconds later (Murray & Cox, 2004b).

During the 1970 flight of the Apollo 13 spacecraft (at 200,000 miles from Earth and moving away at 2100 miles an hour), the crew transmitted a report of a major technical problem—a life threatening fault—back to the Mission Control Center in Houston, Texas. The Mission Control organization then

> began the emergency procedures that grew into an effort by hundreds of ground controllers and thousands of technicians and scientists in NASA contractor plants and on university campuses to solve the most complex and urgent problem yet encountered in space flight (Woodfill, 2004).

The problem was a power reduction in one of the two main electrical circuits ["We've had a main B bus undervolt" (Lovell, 1970, quoted in Murray & Cox).] that created a threat to the computer-controlled Command/Service Module—an information security problem.[5] The computer that controlled the critical infrastructure systems on the spacecraft was losing electrical power, and the time was limited for finding a solution before all systems would fail. While this was not a malicious attack such as a date / time logic bomb planted by a disgruntled worker, the result was the same. An unexpected malfunction placed the computer systems at risk of failure if a solution could not be developed in time. The dramatic and ingenious remedies applied by the crew in concert with ground-based experts saved the lives of all three members of the crew. Even though

[5] A threat exists when there is an agent that places a system vulnerability at risk of exploitation.

Apollo 13 failed in its mission to land on the moon, it was acclaimed as successful because the manual engineering of the spacecraft brought the astronauts safely home.

The existence of the *Y2K* bug in the computer systems of critical infrastructure organizations prior to the year 2000 created a similar time-limited emergency. The emergency was managed and resolved successfully through the work of a large number of individuals and organizations. One of the organizations that achieved notable success in this effort was Delta Air Lines (Delta). The successful elimination of the vulnerability at Delta provided a model to investigate how organizations contend with problems affecting the security of electronically stored and transmitted information, and how context influences their solutions. Like the threat to the Apollo 13 computer system, the risk posed by the *Y2K* bug to aircraft and crew in Delta's flight environments was a central concern. However, commercial airlines are not flying in the emptiness of outer space, but within an airspace that is overcrowded and continuously changing. In addition, the institutional entities that work to insure the safety of all passengers and aircraft had *Y2K* problems of their own. In Delta's case, like Apollo 13, the swift and well-ordered processes of a complex collection of entities averted the catastrophic consequences of the information security vulnerability. Similarly, Delta's interventions were hailed by many as bold and innovative and set the mark for other organizations by their achievements. Furthermore, in contrast, the potential consequences of *Y2K*-related failures in terms of loss of life and property made the Apollo 13 issue seem like a walk in the park.

Research objective

The objective of this theoretically-based case study was to understand how institutionalized environments influenced information security issues in a large, complex

organization. When this dissertation began, there was an expectation that information security had been compromised at Delta, possibly unwittingly, by the solutions developed during the organization's Year 2000 Program. The notion went further to implicate external interconnections of various sorts in Delta's institutionalized environment. These ideas were reasonable given the history of failures, or at least major difficulties, in large IT projects where external agents were involved, and given the history of implication of outsiders in security breaches of IT systems in large organizations.

Even as this dissertation was winding down, an article in the news described of this kind of vulnerability, albeit regarding an organization unrelated to the air transportation industry (Vijayan, 2006). The article described a security issue allegedly caused by an outside contractor working for the state of Vermont. In the process of performing activities related to the systems work, the contractor accidentally posted the Social Security numbers of hundreds of health care workers online. Similar incidents had been in the news for years; therefore probing a bit at Delta would certainly find such evidence there.

There were two major reasons that the original notions about external influence came into focus from an academic perspective. First, prior studies—about normal accidents, unanticipated results from planned activities, garbage can models, and ideas pointing to a "dark side" of organizations—led to a theoretical forecast whereby in the predictable chaos of a large, critical, multi-faceted, time-delimited project, not everything would come to pass as an organization would desire it, no matter how well it was planned. The expectation was that in the institutionalized environment in which Delta lived, outside complexities would compromise information security in unexpected ways.

Second, it is usually the case when working on code in an organizational setting that myriad issues come to bear on its efficiency and effectiveness at any point in time. Just imagining what could happen in an attempt to reconcile technical issues with hundreds of application systems, undergoing modification by a number of programmers (maybe from outside contractors), in a large, complex organization within a short time frame was cause for trepidation.

However, along with envisioning success for these propositions came the recognition that organizations are disinclined to discuss issues related to information security for the obvious reason of fear of inviting compromise—to systems, or reputation, or both. Therefore, the subject had to be approached with caution and with concern for the organization's perspective. Reasoning that by investigating a successful information security event that was fading into history, and by declaring the intent to illuminate the involvement of external "culprits," the confidence that Delta would not be reluctant to participate was established.

Experience has born out some but not all of these preconceived notions. It is true that the organization was a receptive target. Delta's executive management was very supportive of the investigation; however, many other Delta employees were cautious about contributing to the research, and not all (if any) of their reluctance related to concern for security vulnerabilities. Given the state of Delta's financial condition in 2004 when the study began, most concerns related to job security or the possible negative impact on future employment.[6]

---

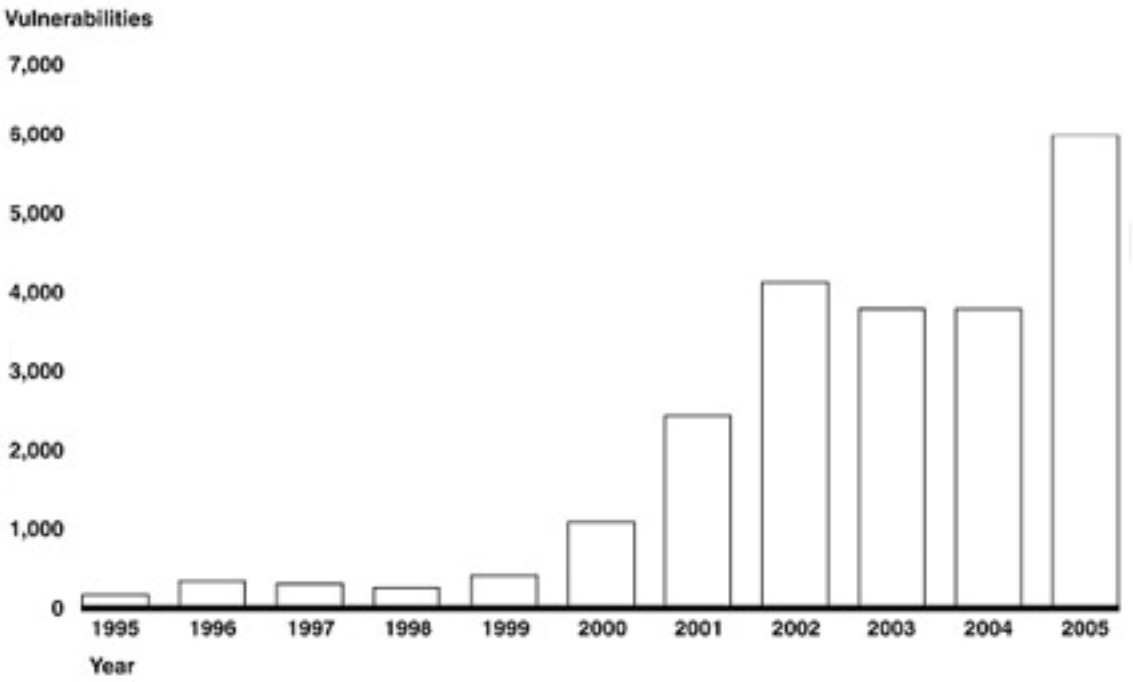
[6] The company had cut 13,000 employees, or 16 percent of its work force, in 2001.

It is also true that Delta's Year 2000 Program was complex. Complexities related to their financial condition had been evident in the Delta organization for over a decade; and especially notable were the complexities in the organization's struggles for leadership; and in its IT systems. Indeed, it was also true that Delta's external environment was the source for compromise to information security, but not in the way that was envisioned. The role of Delta's industry environment was surprisingly one of cooperation and support among the regulative entities in air transportation rather than the adversarial and inflexible positions that were expected. It was the technologies themselves and the institutional arrangements that surrounded them that ultimately set Delta up for information security issues.

Information security vulnerabilities and threats

By the late 1990s, threats to information security had become a critical issue for the U.S., and for the global community of computer users, with no clear understanding of how to combat them. Historical evidence had shown that both a growing reliance on computer-based systems and their pervasive use had created new vulnerabilities as well as multiplied the threats to organizational assets and infrastructure systems. The number of malicious attacks was increasing along with the growing number of vulnerabilities. In year 2000, the CERT® Coordination Center (CERT/CC) received 1,090 reports of security vulnerabilities.[7] Figure 1 shows the dramatic rise of reports in the following years.

[7] The CERT®/CC, based at the Carnegie Mellon University, is federally funded and functions as a central information exchange repository.



Source: U.S. Government Accountability Office (2006).

Figure 1: Security vulnerabilities, 1995-2005

In the instance of *Y2K*, an information security vulnerability of unprecedented scale, a vast number of organizations had tackled and resolved the problem, even as their networked environments complicated the process. A small detail written into the code of computer-based systems before the year 2000, often called the "*Y2K* bug," had emerged to create a worldwide crisis. At best, the *Y2K* problem represented a potential interruption to the normal workflow of an organization. At worst, the problem jeopardized the reliability and the ultimate safety of critical infrastructure operations worldwide.[8]

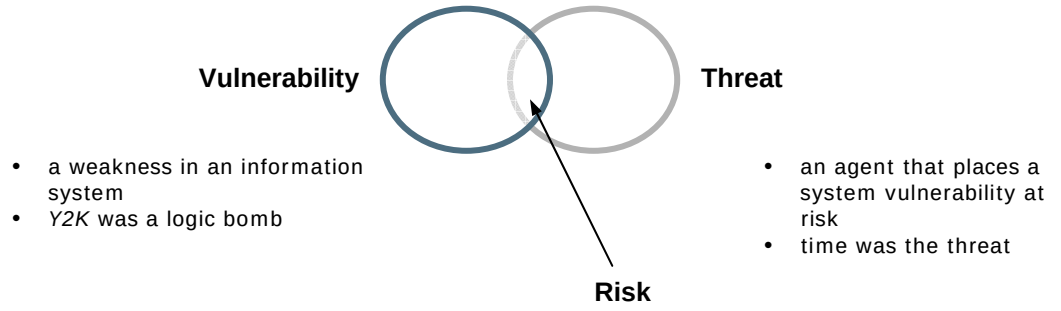
Global resolution of this problem by its year 2000 deadline was extremely expensive; yet in comparison, the problem was a microcosm of the security problems that

[8] According to PDD 63, "Critical infrastructures … include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private" (U.S. Department of Justice, 1998).

remained. The importance of the experiences illuminated by this case is Delta's success in organizing and executing to repair critical flaws in IT systems under very complex circumstances. The case is exemplary because of the efficiency of the cooperation and coordination within the air transportation environment.

Perspectives on information security management

A great deal of dialogue lately has concerned the varied and conflicting perspectives regarding information security management; and organizations have been the focus of much of the discussion. The problem is one of risk management, and may be called a *wicked* problem because it cannot be solved (Rittel & Webber, 1973). It is a process involving trade-offs—a process of understanding vulnerabilities and threats, and applying adequate controls (See Figure 1). As vulnerabilities change, and / or as new threats are discovered, the controls must adapt in order to maintain adequate security. In the volatile setting of a networked system, there is continuous monitoring and evaluation of threats, discovery of vulnerabilities, and re-evaluation of controls. The more a user can understand the vulnerabilities of the system, the better s/he can control for known threats. Increasing the complexity of the systems and the changing nature of threats add to the difficulties of the challenge.



Source: M. Nelson-Palmer, Georgia Institute of Technology

Figure 2: Information security is a risk management process

To improve the management of information security, many practitioners and academicians have advocated a holistic approach, where security strategies include deliberation and input from the entire organization, as opposed to the more traditional and limited view from within the IT department. A holistic approach promotes activities such as increasing the awareness and the understanding of security vulnerabilities in organizations and the improvements such awareness can bring. However, information security is a subject that not many organizations want to highlight. In fact, many organizations believe that increasing general understanding of security vulnerabilities can not only result in adverse publicity but also bring evildoers to their doors.

Such topics of discourse revolve around the existence of non-technical factors that affect security in organizations in ways not studied in the past. Non-technical factors include cultural beliefs and attitudes, norms of behavior, and other social constructions that influence security actions, such as ways of organizing or regulatory policies. Historically, efforts to improve the security of computer-based systems have focused on technical system components, i.e., hardware and software. Researchers and practitioners

now recognize the strong interaction between technical and non-technical aspects of the problem, and understand that the non-technical aspects are significant. The non-technical aspects are viewed now as equal to if not more important than the technical problems; in fact, the non-technical problems are impossible to eliminate. Further, those non-technical aspects that exist at the external environment level (i.e., outside organizational boundaries), are especially difficult to manage. However, this does not mean that efforts to deal with non-technical factors should be abandoned. To the contrary, it means that new and more insightful ways to view the problem must be developed in order to improve methods of protection. Information security can and must be improved.

During the crisis of *Y2K*, both technical and non-technical factors, inside and outside organization boundaries, influenced organizations to renovate information systems in particular ways. The technical environment (i.e., the technologies) could be implicated as the determining cause of certain conditions and behaviors in the workplace. However, social scientists have always been skeptical of such arguments, their point being that technologies by themselves cannot be the independent cause of anything. It is not the technologies alone but the manner in which the technologies are applied, reflecting the motives and actions of individuals and groups that control the technologies. Examples of known non-technical influences on information security decisions within an organization are the knowledge and skills of its members, management involvement, risk communication, types of work organization, policies, setting, etc. Less understood are the influences that originate outside organizational boundaries, especially those that can be characterized as institutional. As consequences of these non-technical types of influences, both similarities and differences likely existed among the security solutions of the great

variety of complex organizations that staged a *Y2K* project—even though the *Y2K* bug had immutable technical characteristics. This dissertation has investigated the activities inside one of these complex organizations. By investigating the impacts of institutionalized environments on the Year 2000 Program at Delta, an opportunity existed to learn more about these non-technical aspects of security problems.

Research question

The question was, *how did Delta go about addressing and solving an IT problem that affected the security of its electronically stored and transmitted information, and how did contextual conditions influence its solution?* This dissertation examined the process by which Delta, a complex critical sector organization and one of the nation's oldest commercial air transportation organizations, dealt with the crisis of *Y2K*.

The crisis of *Y2K* was created by vulnerability in computer code. Many computer-based systems containing date calculations had been developed using a two-digit code, rather than four, to specify the year. Because of the uncertainty regarding date calculations beyond 1999, no one knew whether systems would create erroneous results or fail completely without remediation or replacement of the lines of code that contained the *Y2K* bug.

The crisis of *Y2K* was a massive information security confrontation that required "the largest concentrated effort ever undertaken [by Delta]" (Delta archive, "Mission Year 2000 Master Plan, Section 1.0 Executive Summary," 1998, p. 4). In order to manage the remediation/renewal program, in 1996 Delta set up a Program Management Office (PMO) that included, among others, a representative from every business area of the organization. Its strategic plan for eliminating the security vulnerabilities associated with

Y2K included specific activities to be performed in each business area. However, this plan lacked momentum; and toward the end of 1997, Delta was under pressure to deal with the *Y2K* bug.

In that same year, in addition to the focus on the *Y2K* bug, Delta "launched a companywide Information Technology (IT) Transformation process," with a stated goal "to simplify the technological infrastructure, improve efficiency and deliver state-of-the-art solutions for Delta's business needs" (Delta Air Lines, 1997, p. 15). Between 1997 and 2003, Delta's IT organization (i.e., *Delta Technology*) inventoried and assessed its IT systems, designed a new "transformed" systems architecture, and implemented changes both to its organization structures and activities and to its IT systems—all activities that were intertwined with solving the organization's *Y2K* problem. However, as one might expect in a complex organization, these changes were not uniform across the organization; instead, they represented a variety of solutions across the business areas. Across business areas, some solutions were similar, but also some were different. Drawing from Delta's archival records, interviews, secondary sources, and a review of the literature, this dissertation employed an organizational system model an attempt to explain what happened and why.

Structure of the investigation

The following questions established the structure of the investigation: *which of two models of an organizational system offers a better explanation for the variation among the Y2K solutions of Delta's business areas? Based on the evidence, does an institutional system model or a rational-contingency system model provide a better fit?*

Further, in developing the model, can environmental conditions be identified as specific factors that contributed to the diversity of solutions in the Year 2000 Program?

If an institutional system model fit the evidence, then this dissertation could verify and replicate in the context of the Delta setting the generalization that an organization performs based on other than rational preference (cost/benefit) criteria. It could also demonstrate that institutionalized environments are important to information security management. Institutional theory has been a useful rubric for explaining decisions in organizations that cannot be explained by rational choice models. By connecting environmental factors to decisions, institutional theory has explained why organizational output deviates from what is rationally designed. Even though technical procedures may be rationally planned, evidence has shown that cultural and historical forces, and other regulative structures, may control ultimate outcomes. (Theorists argue also that the behavior of *individuals* who work within large established organizations can become institutionalized.[9] The supportive structure and routines can lead to a narrowing or reduction in critical judgment and reasoning. This mental outlook can lead to oversights and slowed reaction to changes outside the organization thus hindering adaptation to new circumstances.) An institutional system model conceptualizes an organization's technical processes as constructed from within a social framework (e.g., organizational structures), which in turn is shaped by cultural and historical pressures and institutional environments.

Institutionalization, particularly evidenced by field-wide adoption of organizational structures and practices, occurs in all types of organizations and affects

[9] Using a broad definition, institutionalization refers to an acculturation process, the social integration of an organization with its surrounding culture that develops over time.

organizational output.[10] Institutionalization is a result of routines and of shared environments, environments that present cognitive, cooperative, competitive, and coercive means to influence thinking and performing.[11] Given the importance of computer-based information and communication technologies to the functioning of modern organizations, many, in fact, propose that coercion is required to improve security and recommend laws and regulations that can apply within the organizational setting. Paradoxically, computer-based communication and operation are constrained and channeled in ways that derive from laws, rules, and practices designed for organizations, but that may actually impede organizational effectiveness as well as adequate security management.

Overall results of *Y2K* for Delta included not only the elimination of the *Y2K* bug, but also updated software systems and equipment that produced gains in processing accuracy, productivity, and efficiency. However, among its four core business areas, outcomes varied in scale. The *Airport Customer Service* area replaced almost everything, as CIO Charlie Feld said, "Plow the field, and replace." The other three areas—*Operations* (aircraft and crew), *Business Support* (accounting, finance, HR), and *Revenue* (sales and marketing)—remediated code prior to the rollover, but later replaced a number of systems with commercial off the shelf (COTS) applications. In the *Operations* area in particular, Technical Operations (Tech Ops) made a huge investment in COTS ERP (enterprise resource management) systems after the *Y2K* crisis had passed. This dissertation examined these *Y2K* compliance solutions by analyzing the four business

[10] An organizational field consists of communities of related organizations: organizations that produce similar services or products together with their suppliers, resource and product consumers, and regulatory agencies.

[11] Cognitive refers to mental processes of knowing, thinking, and learning.

areas as embedded cases in order to understand: *What caused the differences in approach to Y2K solution? If all business areas had the same technical problem, and the Year 2000 Program was managed as an organization-wide effort with the same mission, how did the different results come about? Further, upon reflective analysis, were the various remedies the best choices with respect to information security management?*

This dissertation sought to answer these questions by investigating non-technical factors in the specific business area environments that may have contributed to the diverse technical solutions. One might speculate that the *Y2K* team in each business area chose the most rational and efficient route to dispose of the problem, and that efficiency meant different solutions within different business areas. One might speculate also that solutions could be described as incremental changes, representing modest alterations to existing information systems, which were dissimilar among business areas. However, investigation of this dissertation was focused especially on institutional aspects, including how institutional manifestations may have varied with respect to differences in the institutionalized environments of business areas, i.e., sector histories with respect to culture, regulation, and computer processing, and associated best practices.

The attempt to locate determining sources of variation involved sorting through a number of complexities. The investigation began with the central assumption of a tendency toward isomorphism within the respective fields represented by Delta business areas.[12] Initial questions included, *what were the specific solutions in response to the Y2K problem in each setting? How was each business area setting organized? What*

[12] Isomorphism is a process whereby organizational characteristics diffuse within a field to create more similarity among organizations over time (Scott, 1992, p. 209).

organizational cultures existed? Did business areas deal with dissimilar regulatory requirements, or other specialized institutional rules or practices, or something else?[13]

Importance of the dissertation

Answers to these questions were important for several reasons. First, by revealing the influence of institutional context on *Y2K* compliance approaches, this research had the potential to demonstrate the value of an environmental-level approach to information security management, i.e., consideration for ways of improving security management through environment-based mechanisms. Next, it could reveal ways in which institutional environments shape organizational structures and processes. Thus, this empirical investigation allowed examination of hypotheses with respect to information security that theorists had generated about institutional influences in general and therefore might be of interest to social scientists.

The dissertation sought also to contribute to the field of public policy. It examined information security in organizations as an important societal issue that was timely and critical to organization survival. In addition, because of the global nature of networks and the e-commerce environment, the issue transcended national boundaries. Therefore, the dissertation's focus on environmental influences could contribute to understanding on the part of public policy-makers who face decisions that impinge on the entire global policy space. Further, the structural similarities of public and private organizations, and their common utilization of networked information systems, make this research of potential interest to managers in all types of organizations, in addition to information security

[13] Institutional theory claims that patterns of organizational interaction and adaptation develop in response to social and cultural environments. Such patterns, even if supportive of an organization's primary mission, may not contribute favorably to maintaining adequate security.

researchers. Indeed, all users of information technology—as individuals and as organizations—have a stake in providing for the security of the network commons. Therefore, increased understanding of the process of improving information security management in organizations is important and useful to consumers and to the public-at-large.

Finally, as is true with any initial effort, likely there were both mistakes and improvements made via the Year 2000 process. Analyzing the effort and debriefing participants offers decision-makers the opportunity to understand factors that affect the safety of critical infrastructures. If, on the one hand, this research effort could show that laws, regulations, industry guidelines, or other institutionalized patterns were at odds with the *Y2K* problem solution, the analysis could provide direction to correct these issues. On the other hand, if structural systems were harmonious, this knowledge could be used to add confidence and strengthen efforts to improve information security management.

Organization of the dissertation

This dissertation is organized as ten chapters. This chapter provides overview information on the current information security problem, and the structure of this investigation. The overview presents background information paying particular attention to organizations' dependence on vulnerable information networks, the social conflicts in information security management, and the difficulties that abound in the current security terrain. The chapter also describes a bounding framework for organizing the information security literature. Chapter 2 is a literature review, which reflects both the information security literature and the organization theory literature that supported the arguments of this dissertation. Chapter 3 presents hypotheses about how institutionalized environments

influence information security solutions and the design for the investigation. The chapter outlines the approach to addressing the research question, and explains how this approach addresses both the empirical problem and the gap in the information security literature. Chapter 4 describes the sources of evidence and the research method, which is a cross-case comparison of organizational and environmental characteristics and *Y2K solutions* among four Delta business areas. Chapters 5 and 6 provide background on the Delta organization and the Year 2000 Program, respectively, which represented the common context for the case studies. Chapter 7 describes and analyzes the environments and solutions at the individual sub-case level and presents metrics from *Y2K* assessments in each case. In Chapter 8, these solutions and contexts are compared across business areas. In Chapter 9, events and outcomes related to information security following the rollover of Year 2000 are discussed. Chapter 10, the concluding chapter, presents a summary of findings, a discussion of the limitations and theoretical implications of this dissertation, and practical ideas for information security management. The next section begins the overview discussion of the information security problem.

Overview of the information security problem

> We are now using our most novel, fragile, and vulnerable infrastructure to operate and coordinate all of the others. There is no part of our social and economic infrastructure that is not operated by our telecommunications infrastructure (Murray, cited in Parker, 1998, p. xii).

Critical infrastructure systems: a growing concern

Our economic and social well-being depends on the reliability of computer-controlled infrastructure operations and the global networks to which many are connected. In the past, infrastructure organizations were relatively distinct, autonomous,

and had few interconnections. Now, thanks to computer-based systems, all of these organizations represent a proliferation of complex interconnections and interdependencies. While the extensive reach of such networked environments adds enormous productivity and operations control benefits, it also adds complexity and increased vulnerability. The global nature of the Internet and its common use by millions of individuals and organizations worldwide raises the risk of interruption or damage to information systems.

Failures in critical infrastructure systems—such as the August 2003 blackout in the Northeast and Midwest; and network breaches that disabled Bank of America's automatic teller machine network, interrupted a nuclear power plant network in Ohio, and the operations of CSX Corporation trains and Continental Airlines flights (Berlind, 2003)—not only confirm their importance, but also reveal their vulnerability. The *Y2K* bug—the systems code that had become a standard programming practice—had the potential to generate events with similar grievous outcomes in vitally important systems. These happenings foreshadow what could happen in an intentional security breach designed to cause harm.

Among the public, a common concern about information security is a system breach that could result in theft of valuable personal or corporate information.[14] Yet, security breaches also may include the corruption of information, a condition with less evidence of public consideration. Destroying the integrity of processed, stored, and/or transmitted information can impair its accuracy and thus interrupt business activities, and

[14] "Identity theft topped the list of consumer fraud complaints to the Federal Trade Commission [FTC] in 2003… the commission estimated that identity theft hit 9.9 million victims in 2002 … as many as 27.3 million in the last five years" (McGuire, 2004).

critical control functions. The availability of accurate information helps an organization to control and coordinate its internal and external activities and relationships, and influences its effectiveness. The potential for corruption of information, and its implications for critical infrastructure systems, was the chief security issue of *Y2K*.

Corruption can originate from various acts: accidents and mistakes; and criminal misconduct, such as corporate espionage, propagation of viruses, denial-of-service attacks; and even cyber-terrorism. While some have discounted the idea that a network attack can actually damage physical objects (Lewis, 2002), others have written about the real possibility (Byers, Rubin, & Kormann, 2003), and have pointed to events characterized as cyber-terrorism that have already occurred.[15] Goodman, Hassebroek, King, and Ozment (2002) suggests if we cannot find answers within a few years, criminals will use computers as instruments to bring about enormous physical damage. Taking into account the continuation of computer crime and other threats to critical systems, it is essential to better protect and defend against computer-based attacks—and to provide safety features to guard against other failures.[16]

Non-technical factors in information security management

Even though maintaining technical systems is a very important part of managing security in networked systems, non-technical aspects are important as well. Managing security with respect to non-technical aspects involves managing unresolved social

---

[15] In 2001, a Queensland man was found guilty of using his car as a command center to sabotage the computer that controlled a sewage treatment plant (Osborn, 2003). In 2003, a teenager is alleged to have brought computer systems to a halt at the Port of Houston, in Texas, from his bedroom in Shaftesbury, Dorset, in what police believe to be the first electronic attack to disable a critical part of a country's infrastructure (Allison, 2003).

[16] A threat exists when there is an agent that places a system vulnerability at risk of exploitation. This work limits focus to the human agent, apart from natural causes (e.g., weather related damage).

conflicts and other obstacles, both within organizations and in the larger social environment. While organizations want to protect information in their systems from technological accidents and criminal misuse, they also want to permit reasonable access to information for those who are authorized to use it, and to maintain adequate privacy of information that belongs to individuals and organizations. Obstacles to achieving these goals exist both in dealing with complex, changing technology, and in the political environment. Thus, social or non-technical factors complicate the technical challenges.

In the U.S., especially, information security is affected by unresolved social conflicts. All organizations face decisions about the best ways to use and to protect their systems, and about the amount of staffing and funding needed to enable adequate security. However, complicating this decision process is a tension between individuals and organizations. Individuals want the advantages that using computer-based networks provide; and they want their personal information protected. Yet, information privacy cannot happen without effective security. Furthermore, any advantage of network use, such as customized information and online transactions, jeopardizes the security of their information. Organizations also want to use computer processing and network transactions to their advantage—to make their operations more efficient and to acquire competitive position. A secure environment that supports integrated, enterprise-wide information systems is important to processing accuracy.[17] In addition, increasing competitive position through management of supply chains and e-commerce requires essential focus on security. Especially in online environments, concern for public image motivates attention to security. Organizations want to be viewed as responsible, reliable,

[17] It is difficult to achieve and confirm data accuracy with disparate internal systems, possibly incompatible for network connection.

and trustworthy; therefore, they value systems security and other attributes that promote this image. In contrast, organizations operating in the competitive environment of cyberspace also want to use the personal information of network users and customers in ways that can increase their revenues and their competitiveness. Many customers view this as *ir*responsible, *un*reliable, and *un*trustworthy—as exhibiting behavior that is unethical and unconstitutional.

The role of government is another source of conflict in the process of providing information security.[18] Neither individual citizens nor organizations are eager for unauthorized use of private information, or for government surveillance of private electronic transactions that would assist in tracking criminals. However, the government's national defense community, as well as standard law enforcement, has need for surveillance capability (Denning, 1997). While there is consensus that networks' vulnerability to fraud, theft, and other disturbances should be reduced, the methods that public agencies recommend for tackling the problem are fraught with problems.[19]

These conflicts reveal the challenge for information security policymakers in determining an acceptable balance between freedom and order. Just as we need to increase the security of information systems—improving the confidentiality, integrity, and availability of information—by providing controls to mitigate malicious acts, normal accidents, and mistakes, we seek to improve the usability of systems while maintaining the privacy of individual and organization information.

---

[18] Incidentally, public organizations face many of the same concerns as private sector organizations about the aforementioned and other security issues.

[19] For example, many involved with intelligence and law enforcement argue that identifying terrorists requires enhanced access and use of information. However, the use of corporate databases containing personal information on individuals in an effort to identify terrorists has been met with criticism from those who see such measures as a threat to privacy.

Proper prescription for information security ailments can only happen after first reconciling the discrepancies between the goals of individuals and organizations. An institutional infrastructure must be coordinated among social, organizational, and political rule systems. As part of this process, structures at a societal level—cultural, economic, and political—must all adapt and integrate new information into an established institutional system of values and functions. Then organizations can improve information security management with a clearer understanding of how environments influence the behavior of individuals and organizations, and how those influences ultimately affect IT systems and the security of their information.

Obstacles in the security terrain: complexity, change, and politics

Researchers and practitioners have developed and implemented numerous approaches for improving systems security, but reports of both malicious exploitation of information networks and other system malfunctions confirm that networks remain vulnerable and that the intrusions are taxing human ability to respond. The financial losses to organizations have taken a heavy toll (Richardson, 2004). These reports have shown either that we have not discovered the optimal combination that works to protect systems adequately, or that perhaps approaches have been prescribed without first properly determining an organization's essential requirements. Major obstacles in the security terrain are systems complexity, rapidly changing technologies, and complications in the political arena.[20] First, consider the issue of systems complexity. As

[20] A report by the NAS Computer Science and Technology Board (National Research Council, 1991) attributes the "computer security problem" to the rapid pace of technological change, the slow pace of government interventions (through procurement and evaluation programs), export controls, a lack of consumer understanding of the risks, and the limited recourse that U.S. users have against vendors of flawed software.

computers have become more powerful and organizations have become more diverse, people have designed systems that are more complex.[21] Failures in large technical systems—so-called "normal accidents"—have been attributed to complexity (Perrow, 1984; Petroski, 1994; Sagan, 1993). A quick analysis of large system failures usually results in blaming the operators. Often, however, while operator error is the most direct source, the real culprit is the unexpected or unforeseen consequences of complexity.

A second obstacle in the security terrain is rapidly changing technologies. The past few decades have seen a tremendous increase in both the breadth and complexity of computer-based systems. As the fast pace of technology development continues, vendors hurl complex application software and advanced hardware on the market without standards or adequate testing. It is difficult for users, including systems administrators, to keep up with changes in the products that have been released and employed.[22] Security patching, program configuration, and other security-related activities require relentless effort. One may speculate in the case of *Y2K* that the technologies were so difficult to maintain and the changes were emerging so rapidly that it became difficult to stay abreast of changes. Did the snarl of change management eclipse the date problem?

Finally, failures in large technological systems are associated with not only human practices and mental processes, but with broader social structures such as culture, communication, and politics (Cohen & Noll, 1991; Klein, 2000; Vaughan, 1990).[23] Klein suggested that conflict between coalition politics and program administration can explain

---

[21] Evidence of systems complexity is the enormous amount of effort and expense required in the *Y2K* compliance process, eliminating a small piece of technical code from IT systems.

[22] Ironically, increasing homogeneity in hardware and software also makes information technology (IT) more vulnerable. Consider the widespread use of Microsoft Outlook and the TCP/IP protocol. These products have enabled the propagation of viruses, worms, and Trojan horses, often called malicious software. [Note: Referring to malicious software, Schneier (2000) calls this "malware" (p. 151).]

[23] The *Y2K* process involved all of these societal structures.

failures in large, complex systems development programs. Political forces common to most programs create three general offenders, any of which can contribute to system failures: geography, multifunctionality, and budgetary uncertainty.

These technical, political, and fiscal obstacles are formidable. However, even if we were able to exclude them, we cannot make such systems completely reliable and secure because of the restrictive user environment this would create. Using information systems requires human interaction, which means accessibility. The human contribution to the problem, the "user access," is a large part of its intractability. Information security requires a careful balance between user access and information safeguard (McFadden, 1997), in addition to balancing risk and expenditure (Schneier, 2003). Social norms, regulatory structures, organization culture, cognitive processes, and the presence of other organizations influence user behavior within organizations. We need to understand those parts of the problem better so that we can minimize security incidents and avoid catastrophic failures.

Uncertainty and complexity are evident both in the problem space of information security, and in the way that stakeholders want the problem addressed. Such conditions create problems for action; both organizations and individuals lack the conviction that enables decisive direction. According to Turner (1976), "Action is made possible in organizations by the collective adoption of simplifying assumptions about the environment, producing what Simon (1976) called a framework of 'bounded rationality'" (p. 378). It is imperative therefore, that empirical effort be guided by a bounding framework that promotes clearer understanding.

A conceptual framework for literature in the information security field

A conceptual framework incorporating four dimensions organizes the information security literature, and exposes gaps where further research is needed. The four dimensions are organization, environment, technical, and non-technical. While these dimensions are not the dichotomous variables represented in the framework, they are presented in this form as an aid to broad classification. Positioning these dimensions as a matrix (See Table 1), the technical-organization quadrant contains the bulk of the academic literature on information security. The remaining three quadrants hold the relatively fewer and more recent works.

Table 1: Framework for information security literature

	TECHNICAL	NON-TECHNICAL
ORGANIZATION		
ENVIRONMENT		

On the horizontal axis, the framework segments the information security research into two areas of focus, predominantly **technical** or **non-technical**. On the vertical axis, the framework further divides the research depending on its **level of application,** either **organization or environment**. That is, does the research relate to information security from the perspective of an organization and its internal activities or from that of an

organization as it spans outward to its environment, such as to the marketplace, sectoral environment, or socio-political system?[24]

Summary

This chapter introduced the research problem, the research question, and the context of the broader information security landscape. The information security landscape was presented in three sections, paying particular attention to organizations' dependence on vulnerable information networks, the social conflicts in information security management, and the difficulties that abound in the current security terrain. A fourth section described a bounding framework for organizing the information security literature, designed to expose gaps where further research is needed.

[24] One aspect of organizational environment is its "technical," or "task," environment, which refers to sources of "material [resources], technologies, and information essential to the transformation of inputs into outputs" (Dill; Thompson, cited in Scott, 2000, p. 1). Environment also refers to social, political, and cultural influences on behavior. As a third aspect, direct association to the natural environment was excluded in this study.

CHAPTER 2

WHAT EARLIER WORKS HAVE CONTRIBUTED

> The essence of good security engineering is understanding the potential threats to a system, then applying an appropriate mix of protective measures—both technological and organizational—to control them (Anderson, 2001b, p. xx).

This chapter reviews the information security literature using the four-quadrant framework that was developed in Chapter 1. Applying this framework, the organization-environment quadrant reveals a gap in understanding of the information security problem. Following the review of the research domain of information security, the literature of organization studies is presented in this chapter as a way to build knowledge in this area.

Information security literature

Table 2 positions topics within the literature-organizing scheme described in Chapter 1. The leftmost two quadrants contain a non-exhaustive list of topic areas in the literature focused on technical information security, that which concerns strictly hardware and/or software-related issues.[25] A review of this research revealed that problems continue to shadow technical strategies, such as access control (including defense against malware) and software development methods. Software developers have difficult problems, not the least of which is that both distributed systems and security principles are relatively recent additions to their work (Anderson, 2001a). The continual discovery of software bugs (only revealed through attacks that exploit them), has substantiated the need for improvement in this area. In addition, many technical strategies have been detail

[25] This review does not identify specific work in the technical area. Because of the focus of the study, discussion is limited to literature related to non-technical topics.

intensive and have required tailoring to a specific system and continuous vigilance to insure that systems are properly fortified. Such methods have invited problems because of the attention required (Goodman, Hassebroek, King, & Ozment, 2003). Turner (1976) has described these methods as a way of circumnavigating an ill-structured problem. System administrators must stay highly motivated for these methods to be effective.

Until recently, the literature defined information security only by the technical aspects of the problem. The literature has proposed technical changes for managing systems, but neglected the human aspects. Different from a technical perspective with its focus on hardware and software, a non-technical perspective relates to the reciprocal nature of the relationship between people and systems. A non-technical perspective views people as the designers and users of the systems, and therefore, as the instrument for security management. A non-technical perspective includes consideration for organization context, including both its institutional and its task environments, which is related to human motivation, responsibility, and ethical decision-making. An illustration of the technical and non-technical nature of information security management is the pilot program announced in 2004 by the Transportation Security Administration (TSA). The TSA plan described employing technical systems to improve the security inspection of airline passengers (Verton, 2004). Biometric systems, such as fingerprint and iris scanners, were the foundation for the authentication system, together with an IT network component to integrate this information with a TSA database. However, providing adequate security using this system entailed not only designing the technical features, but also required a non-technical component: the project required structures and procedures for people to administer the systems and to analyze and evaluate results.

Non-technical topics in the information security literature are shown in the rightmost two quadrants of Table 2.[26] This literature is largely conceptual in nature with little evidence to support the ideas. In addition, those empirical studies that do exist exclusively relate to activities internal to an organization, the topics shown in the upper right quadrant. This review briefly discusses those studies. Following this discussion is an overview of published ideas in the non-technical-environment category, the lower right quadrant that contains this dissertation.

Table 2: Classification of information security literature

	TECHNICAL	NON-TECHNICAL
ORGANIZATION	Access control Defeating malware	Agents -actions -motivations Organization -culture and training -security strategy, policy process -security controls
ENVIRONMENT	Systems design and development Macro system control	Interorganizational, national, international aspects -cooperation and collaboration -incentives, channels, and constraints **—This dissertation—**

Studies focused on non-technical factors in organizations

Computer-based information and communication technologies are essential for work performance within modern organizations. However, their reliable functioning cannot be guaranteed because of threats inherent in human-computer interaction. Threats

[26] This matrix classifies research relevant to IT security management. Knowledge—as well as social and economic values and belief systems—dictates approach choices at each grid location. The matrix might also be titled "Strategies to reduce information security risk."

to the security of information in organizational systems exist in both intentional (whether premeditated or opportunistic) and unintentional forms. Intentional system breaches can be brought about by "social engineering" (Mitnick, 2002) and other forms of insider misconduct. Studies concerned with the threat of insider access (CNSS, 1999; Harrington, 1995; Hsu & Kuo, 2003; Leonard & Cronan, 2001; Loch & Conger, 1996; Peace, Galletta, & Thong, 2003) have determined significant indicators for insider-induced systems problems. The collective knowledge from these studies have implicated factors such as individual attitudes, subjective norms, gender, and perceived behavioral controls—maybe an employee with certain situational or personality characteristics who corrupts system operation whether by mistake or by purposely gaining unauthorized system access. In an investigation of the information systems that facilitated ATM fraud in British banks, Anderson (1994) found that "[t]he conventional threat model, of a capable motivated attacker, was wrong; attacks were essentially opportunistic." The study revealed a pattern of losses variously attributed to processing errors, to thefts by staff, or to individuals tampering with the postal service, with system design and operation problems accounting for most of the rest.

Assessing such threats to organizational systems is the first step in the information security process. The next step is to determine the risk in each kind of possible misuse, and to decide how much to spend on control. One obstacle that continues to limit improvement in information security management is the assessment of information security as strictly a cost, instead of as part of the portfolio of risk management issues. The threat and risk evaluation process is vital, and goes hand in hand with an understanding of available control strategies. However, even if organizations use risk

assessment practices in evaluating security investments, when inconsistent values are placed on risk, different organizations will respond differently in their attempts to improve the condition. Ezell (1998) developed a risk management framework that uses probabilistic risk assessment (PRA) methodology to quantify the risks of intentional threats to special purpose control systems. A survey documented information on cyber malfunction, and determined the security concerns of administrators of supervisory control and data acquisition (SCADA) systems in water utilities, in order to find ways of improving robustness, and resistance to intentional breaches.[27]

Understanding the perception of such risk to an organization directly relates to protection strategy. Research surveys separated by over 10 years (Loch, Carr, & Warkentin, 1992; Whitman, 2004) revealed that the perception of threats held by information system (IS) managers over 10 years ago was still prevalent in 2004. Respondents, all senior IS managers, professed awareness of the risk, and believed they were doing well to mitigate it. They believed their organization to be at low risk from viruses, while they believed other organizations to be at higher risk. They were not familiar with state and federal laws concerning computer crimes and believed that their employees and competitors operate in good faith. These findings are significant in that if an organization's threat assessment is inconsistent with reality, the organization will fail to apply appropriate mitigating mechanisms. According to Anderson (1994), "[e]xplicitness is fundamental to robust security. One must be explicit not just about threats, but about how these are tied to mechanisms and how the system will be operated; it is the failure to do this which causes the typical loophole" (p. 37).

---

[27] As a critical infrastructure control mechanism, SCADA systems allow utility operators to monitor and control processes distributed among various remote sites.

Most researchers in the non-technical-organization area have generally supported a holistic approach to security (e.g., Dhillon, 2001; Hitchings, 1995; and James, 1996) and have advocated risk models and security processes that include people and practices enterprise-wide (i.e., not limiting focus to a particular aspect of a component system). This view thus considers traditional ideas of technical information security—assuring confidentiality, integrity, and availability—as only part of the plan. A fundamental element to a holistic approach is alignment of policy for information security with the activities of the organization, making it a part of overall organizational policies. Policy alignment can provide a culture of security that can improve security practices, including increasing awareness.

Designing organization policies that promote reliable, error-free systems is difficult (Anderson, 2001a), but user policies can provide education and structure that affects the security practices of organization members. Harrington (1996) found that providing a code of ethics helped to deter unethical behavior. Peace et al. (2003), a study of software piracy in the workplace, concluded that punishment certainty, severity, and software cost had direct effects on intention toward unethical behavior.

A range of controls can be effective in limiting misuse, including the use of security software and an active security staff that informs users about unacceptable system use and penalties for noncompliance (Straub, 1990; Straub & Nance, 1990). The use of security software has required high-quality systems administration, as improper configuration and monitoring leads to opportunities for insiders to misuse the system easily (Anderson, 1994).[28] Schultz (2002) presented an algorithm that predicted insider

[28] In conjunction with willful misuse, human error is a lingering problem (Wood & Banks, 1993;

threat based on activity logging, but if improper systems management were the problem, administrators would be unlikely to employ such an algorithm.

These strategy issues have underscored the value of senior management to security (Dutta & McCrohan, 2002). While it has long been the practice for management to compartmentalize the IT function, considered a specialized niche operation, management must now view the IT function among the other functional areas that must adapt to environmental pressures (Cannon & Woszczynski, 2002). According to Long (1999), even though many have believed that top management is key to information security within an organization, management generally failed to possess an adequate understanding of security issues and control mechanisms. Straub and Welke (1998) reported similar results from studies in two IT Fortune 500 companies: managers typically were not aware of available security measures.

The theme that came through in the analysis of this body of work was that understanding threats and matching them with effective controls is key to improving information security. However, studies were limited to the internal organization system. If the influences of external environment were not considered, knowledge of either what constitutes a threat or what might be a full range of effective controls would not be possible. A number of initiatives have been developed that focused on organizational environment, but no studies have been performed that would indicate that these initiatives were helping to improve information security management.

Chestnut, 2000).

Topics focused on non-technical factors in environments

Topics in the non-technical-environment category of Table 2 included the cultural, interorganizational, national, and international sphere of information security. Collaboration and cooperation were current themes in this area. Organization self-regulation—the potential for organizations to manage the security of their own information systems, rather than through state intervention—was a focus in this category.[29] Attempting to stave off intervention—and because security management is difficult—industries and professional groups have collaborated in the interest of better tools and practices. While risky to an organization because of the possibility of exposing vulnerabilities in their own systems, sharing information with outsiders has been important for learning how to manage security more effectively. In 2003, the Global Council of CSOs (chief security officers) was formed in order to "share information on Internet security … and to attempt to work with vendors to reduce risks" (Wrolstad, 2003).[30] In civil aviation, the International Air Transport Association (IATA) is an organization of long-standing, with international reach and active information sharing among its member organizations, which includes 270 airlines from 130 countries. Information security initiatives of interest to this global alliance have included using the travel reservation infrastructure as a system for surveillance of travelers, Computer

[29] Private organizations wish to avoid dependency and regulation, which has the potential to limit their autonomy. Limited government intervention has been the subject of a number of publications that observe the advantage of free market development and its effect on innovation, and production (e.g., Werbach, 1997; Neuman et al., 1998; Odlyzko, 1998; Lessig, 1999). The Telecommunications Act of 1996 adopts such a position.

[30] Founding members included Howard A Schmidt of eBay (former White House cyber-security adviser), Bill Boni of Motorola, Vint Cerf of MCI, Scott Charney of Microsoft, Dave Cullinane of Washington Mutual, Mary Ann Davidson of Oracle, Whitfield Diffie of Sun Microsystems, Steve Katz formerly of Citigroup, Rhonda MacLean of Bank of America, and Will Pelgrin of the New York State Office of Cyber Security and Critical Infrastructure. See http://www.csocouncil.org/.

Assisted Passenger Pre-Screening System II (CAPPS-II), US- VISIT, Advance Passenger Information System (APIS), and biometric, radio frequency identification (RFID) on passports and other travel documents.[31]

In addition to private initiatives, a number of organizations have enabled the sharing of information between government and private organizations. The CERT® Coordination Center (the CERT®/CC) and the World Wide Information Sharing and Analysis Center (World Wide ISAC)[32] have served as reporting centers for security incidents. Other ISACs have assembled around critical infrastructure industries and served as community forums.[33] InfraGard is a Federal Bureau of Investigation (FBI) program that promotes protection of critical information systems through information sharing. Its members are required to be U.S. citizens, and must undergo a background check performed by the FBI.[34]

While organizations have attempted to provide confidential settings for discussing security issues, national laws and other regulations make issues public. U.S. federal level policymakers have proposed legislation to provide stronger incentives for organizations to improve their security practices, much as the Securities and Exchange Commission (SEC) provided to publicly-traded companies during the *Y2K* period (Gross, 2003). However, given present understanding of the complex problems that organizations face in

---

[31] After Sept. 11, 2001, Congress passed laws requiring countries in the Visa Waiver Program to issue biometric, machine-readable passports by Oct. 26, 2004. See http://www.wired.com/news/privacy/0,1848,62876,00.html.

[32] Information in the World Wide ISAC database comes from its members, U.S. Government agencies, hardware and software vendors, and other sources.

[33] Internet Security Systems (ISS), a private sector company that provides managed security services (bought by IBM in 2006), hosts the Information Technology ISAC. Airports Council International - North America (ACI-NA) has the role of sector coordinator for the Aviation ISAC.

[34] The Georgia Tech Information Security Center (GTISC) is an underwriter of Atlanta's InfraGard program, the second largest chapter in the country.

addressing security, designing effective federal level legislation acceptable to all stakeholders might be very difficult to achieve.

Legislative efforts were present in the U.S. at both state and federal levels that focused on improvement of security in organizational networked systems. Depending on the jurisdictions within which an organization operated, any successful legislative action required multiple compliance obligations and a legal staff to oversee its compliance. For instance, the Health Insurance Portability and Accountability Act of 1996, commonly known as HIPAA (pronounced "hip' ah"), included provisions that encouraged electronic transactions, but also required new safeguards to protect the security of health information. Other legislative acts requiring compliance, such as Sarbanes-Oxley Act (SOA), mandated various activities to certify business processes that affect security policies for an organization (Bigelow, 1995).[35]

The international character of global networks has prevented total reliance on legal means to influence system use.

> Laws and tax regimes are based on geography, not network topology; online merchants, for example, may be allowed to sell some products in some countries but not others ("Geography and the net: Putting it in its place," 2001).

A consequence of global networks has been the inevitable interaction between U.S. law and that of other countries. Laws to promote security and the protection of intellectual property have differed widely across countries (American Bar Association, 2003), these laws based on cultural differences among other issues. Any nation that has laws inadequate to define and enforce information security has created a safe haven for

[35] The Sarbanes-Oxley law of 2002 mandates that CEOs and CFOs of publicly-traded companies personally attest to the validity of financial statements and other information, and that their companies have proper "internal controls."

network users who would use the network for criminal activities (Goodman, Hassebroek, King, & Ozment, 2003). This situation is likely to remain despite efforts to harmonize laws.

International agreements have involved collaborative and cooperative efforts similar to information sharing, and legal initiatives. International agreements offer the possibility of globally coordinating efforts to share information, track criminals, effect standards, and harmonize the disparate laws of sovereign nations. The Stanford Draft Convention (Sofaer, Grove & Wilson, 2001) proposed a legal globalism for cyberspace. Universal support and ratification of a treaty of this kind helps to eliminate safe havens for attackers. An international initiative of note is the Council of Europe Convention on Cybercrime.

> The Convention broke new ground by being the first multilateral agreement drafted specifically to address the problems posed by the international nature of computer crime (U.S. Department of Justice, 2003).

Although harmonization of laws was just one focus for this treaty, much of the rest of the work depended on this foundation. On August 3, 2006, the Council of Europe Convention on Cybercrime, the first and only international treaty designed exclusively to combat computer crime, won approval from the U.S. Senate, but continued to garner criticism from groups concerned with privacy (McCullagh & Broache, 2006). However, other groups, including the Business Software Alliance (BSA) and the Cyber Security Industry Alliance (CSIA), supported the treaty.

Klein (2002) and "Milton Mueller Delivers Gerbner Lecture 2000" (2000) expressed the notion that Internet Corporation for Assigned Names and Numbers (ICANN) could be effective as an international regime. Mueller stated, "… [T]he creation

of ICANN can be seen as a process by which resource assignment and allocation are linked to [international] regulation and control."

Beyond cooperative arrangements, strategies at the environment-level have included incentives and constraints in the marketplace or political system, often using regulations and policies that required legislative and justice system investments and interventions. Anderson (2001a), Varian (2000), and Schneier (2000) discussed these avenues for improving security management, and advocated empirical investigation. Anderson described the practice of liability dumping by European banks and software companies. In the U.S., banks were responsible for risks in the use of their technologies, while in Britain and other countries, banks defended the "truth" of the information system. In Anderson's view, if the bank carried the risk, then security would become a "straightforward engineering problem." Similarly, software companies were dumping liability on the users. These same works have argued that law should hold organizations responsible for distributing information systems products without proper testing, and that risk insurance should include incentives for adequate organizational security.[36] Varian wrote that insurers want clients with adequate security, which gives insurers incentive to instruct their clients in how to achieve it.[37] "This … illustrates one of the fundamental principles of the economic analysis of liability: it should be assigned to the party that can do the best job of managing risk."

---

[36] The U.S. Senate shelved legislative bills designed to protect corporations from product liability lawsuits stemming from *Y2K* computer glitches (Barlas, 1999). The Business Roundtable CEOs recommended that software vendors incur liability for distribution of insecure products ("Meeting of the Business Roundtable Information Security Coordinating Committee," 2003).

[37] J.S. Wurzler Underwriting Managers requires that an organization demonstrate a certain level of security before providing systems failure coverage (Brush, 2001).

The ideas put forth in the non-technical-environment category were promising; however, they were limited, and largely unexplored and untested. The expansion of focus in information security literature to include such environmental-level social concerns reflected not only the explosion in computer-based communication in recent years, but also the addition of a new global community of users. Thus, not only was a larger, more volatile setting for investigation developing, but also a new perspective on information security.

In summary, this review of information security literature has focused on non-technical aspects, and has provided an overview of research in both the non-technical-organizational and non-technical-environmental quadrants of Table 2. Research in the non-technical-organizational quadrant was focused on activities internal to organizations that affect security; more specifically, the research examined the effects of various internal deterrents to both intended and unintended disruption of information systems within organizations. Conversely, topics in the non-technical-environment quadrant focused on activities external to organizations. In reviewing literature identified with the non-technical-environment quadrant, the shortage of scientific investigation related to this domain was noted. This dissertation helps to fill this gap by applying sociological theories of organization to investigate the effects of institutionalized environments (the social contexts in which organizations are embedded) on information security. Such a guiding framework represents a departure from traditional research disciplines of information security (e.g., computer science).

Theories of organization

At this point one might ask, "Why would we look to theories of *organization* to understand the relationship between *environment* and information security?" The answer reflects central concepts of organization theories: while the primary focus of this literature is indeed *organizational* systems, contemporary theories consider *environment* as a significant component in its influence on organizational behavior.[38]

In order to prepare the reader for a discussion of specific theories, a description of major concepts is provided. The concepts include "organization," "organization boundary," "environment," and, "organization field." The term "theory." is also briefly discussed. Following these discussions, organization theories of interest to this dissertation are introduced.

Acknowledging that many works have proposed differing definitions for the term "organization," this dissertation offers the one that follows as a conceptual grounding for the investigation.

According to Lawrence and Lorsch,

> An organization is defined as a system of interrelated behaviors of people who are performing a task that has been differentiated into several distinct subsystems, each subsystem performing a portion of the task, and the efforts of each being integrated to achieve effective performance of the system (Lawrence & Lorsch, 1967, p. 3).

In order to analyze an organizational system, it is necessary to define the term "organization boundary." Conceptually, an organization boundary separates the entities and activities within an organization from those related to an organization that take place

[38] A "system" is conceived as bounded activity with inputs and outputs. A model described as a "closed system" is separated from its environment, operates within defined limits, and is strictly focused on internal organization activities. An "open system" considers environment as both supporting and influencing an organization. It is reasoned that the more one understands a system, the easier it is to "predict" its behavior. For elaboration of these concepts, see Scott (1992).

in the organization's environment. A definition of the limits or boundary of the organization dictates what is considered the organization's environment. However, complete empirical determination of an organization's boundary is difficult if not impossible. The following is Pfeffer and Salancik's definition for an organization and the limit of its internal activities:

> The organization is the total set of interstructured activities in which it is engaged at any one time and over which it has discretion to initiate, maintain, or end behaviors … The organization ends where its discretion ends and another's begins (1978, p. 32).

Like organization boundary, the term "environment" is equally difficult to pin down. Organization theory literature presents a number of conceptions of the term; however, of these conceptions, four are discussed here. First, as mentioned above, in contemporary theories environment is conceived to be a component of an organizational system. The principal distinction between the concepts of "closed" and "open" systems relates to whether or not environment is considered a component of the system. Specifically, the concept of a closed system eliminates the influence of environment, whereas the notion of an open system incorporates environmental support and influences. Different from early models of organizations as closed systems, contemporary theories encompass various perspectives of organizations as open systems (e.g., Williamson's (1995) transaction-cost economics, Hannan and Freeman's (1977 / 1993) population ecology, Pfeffer and Salancik's ([1978] 2003) resource dependence) in an effort to understand complex organizational structures wherein external environment plays an important role.

A second conception of environment is that it is heterogeneous—composed of various elements that influence organizations in various ways. For example, studies have shown that organizational structure is related to environmental heterogeneity (e.g.,

Lawrence & Lorsch). In order to understand this and various other relationships in an open system model, Scott and Meyer (1983) proposed that the elements of heterogeneous environments be classified as either technical or institutional components. As such, the distinctions between technical and institutional components are not alternatives, but rather represent dimensions that vary in their influence depending on the activities of the organization.

> *Technical environments* are those in which organizations produce a product or service that is exchanged in a market such that they are rewarded for effective and efficient performance (Scott, 1992, p. 132).
>
> Technical environments include production and control technologies, patterns of interorganizational exchange … and other factors that lead to relatively more or less efficient or effective forms of organization (Orru, Biggart, & Hamilton, 1991, p. 361).
>
> *Institutional environments* are characterized by the elaboration of rules and requirements to which individual organizations must conform in order to receive legitimacy and support (Scott, 1992, p. 132).
>
> Institutional environments are composed of organizations that are judged more by the appropriateness of their form than by their outputs. In institutional environments, organizations compete for social fitness rather than economic efficiency (Powell, 1991, p. 184).

In this open system model, both technical and institutional environments channel and constrain organizational performance. For example, the marketplace arena provides a competitive technical environment for resources, therefore potentially constrains efforts to maximize efficient or effective organizational performance. An institutional environment, set within a cultural or political system, establishes social norms and expectations of legitimate behavior, therefore, channels performance depending on restrictions imposed by laws and other social structures.[39] The notion of institutional

[39] A regulation may be assessed in terms of its ability to support an efficient outcome, e.g., tax incentives. However, from an institutional perspective a regulation is a product of a social system, values-oriented and may actually inhibit efficient business operation.

environments is not as well developed as that of technical environments.[40] However, we know that "a clear difference exists between organizational responses to technical and institutional aspects of their environments. … Whereas organizations *exchange* elements with their technical environments, [organizations] are *constituted* by elements drawn from their institutional environments" (Scott, 1992, p. 208). Scott and Meyer (1983) acknowledged that these two environments are difficult to distinguish empirically, but argued that either a technical or an institutional environment must exist for strong and stable organizational forms to develop. For example, airline companies are subject to both "highly developed technical and institutional pressures," whereas manufacturing companies are more strongly technical, and schools and churches are more strongly institutional (Ibid., p. 123). Airline companies must deal with demands for efficiency as well as with procedures related to public values such as personal privacy, safety of individuals, concern for the environment, etc. Moreover, over time, technical processes can become institutionalized as well (Selznick, 1957).

A third conception of environment is that it is dynamic. It is constantly changing, thus re-shaping organization boundaries, and affecting organizational change. Miles, Snow, and Pfeffer (1974) discussed the concept of environmental change as having two aspects: predictable and unpredictable.[41] These aspects influence organizational change or adaptation, but in different ways. Predictable change in environments can be anticipated and responded to in ways that allow organizations to maintain efficient operations. Uncertainty is the aspect of environmental change that creates the most concern.

---

[40] The "institutional" concept is multifaceted and difficult to describe in brief fashion. However, an understanding of what is implied by this term is critically important to this study. The definition is discussed in the section on institutional theory with respect to contributions from a number of works.

[41] Unpredictable environmental change is described as environmental uncertainty.

A fourth conception of environment is that its dimension varies depending on the level of analysis. For example, the environment of a single organization is different from the wider environment of a group of related organizations (Scott, 1992, p. 132). Therefore, either a change in activities or a change in organizational domain would introduce a change in environment for an organization.

As the final major concept, the term "organization field" is used to describe a group of related organizations in a wider organizational environment. DiMaggio and Powell (1983) defined a field as

> those organizations that, in the aggregate, constitute a recognized area of institutional life: key suppliers, resource and product consumers, regulatory agencies, and other organizations that produce similar services or products (p. 143).

According to Scott and Meyer (1994),

> [f]ields identify communities of organizations that participate in the same meaning systems, are defined by similar symbolic processes, and are subject to common regulatory processes. The rationalizing frameworks giving rise to and shaping organizational fields are, in the modern world, constructed primarily by the professions and agents of the state (p. 71).

> Over the centuries, the fields of manufacturing, finance, sales, marketing, and engineering have [each] evolved into a set of commonly understood practices, with established vocabularies and operating principles… (Feld & Stoddard, 2004, p. 72).

This initial grounding is completed by defining the term "theory," and by briefly discussing how organization theory can benefit information security. This is Kerlinger's definition:

> A theory is "a set of interrelated constructs (variables), definitions, and propositions that presents a systematic view of phenomena by specifying relations among variables, with the purpose of explaining natural phenomena (Kerlinger, cited in Creswell, 2003, p. 120).

Theories of organization (specifying relations among variables under specialized conditions and assumptions) explain organizational phenomena; and thus, aid in predicting future organizational performance. It has been said that a perfectly organized

system is completely predictable (Miller, cited in Scott, 1992, p. 84). All uncertainty is eliminated; therefore, there is nothing to learn by observing the performance of this perfect system. In contrast, the performance of a complex organizational system is very difficult to predict. However, "[t]he more disorganized and unpredictable a system is, the more information you get by watching it" (Ibid.). Thus, observing the performance of a complex organizational system during *Y2K* offered the opportunity to discover factors that affected the management of information systems. Organization theories can explain relationships between forces in organization environments and observed actions of organizations, actions that can place the security of organizational systems at risk.

This dissertation employs organization theories in order to explain the diversity of solutions among Delta business areas during the Year 2000 Program. Application of theory offers the opportunity to learn more about the justification for business area solutions in order to predict future outcomes. If this investigation can explain organizational solutions during Year 2000, there is potential for better management of information security in the future, and for providing knowledge that has policy implications.

Two influential organization theories are of interest to this dissertation: rational system theory and institutional system theory. Research efforts within both the rational and institutional schools of thought have sought to explain how and why organizations do what they do. However, the two perspectives present what might be considered competing, even contradictory, views of organizations. Classical rational models of organization operate as controllable machines, attempting to deliver efficient performance and improved effectiveness in such areas as administrative functions,

production processes, workplace structuring, etc. In contrast, institutional models of organization operate as natural systems, social and evolving, a more human metaphor than the mechanistic rational models.[42] Further, institutional models consider manifestations of culture and its shaping of organizational practices.

With reference to rational-institutional differences, Scott (1987) referred to Selznick's model.

> Selznick distinguished between organizations as technically devised instruments, as mechanical and disposable tools, and organizations that have become institutionalized, becoming valued, natural communities concerned with their own self-maintenance as ends in themselves (p. 494).[43]

North (1992) highlights central elements that distinguish earlier theoretical models from more recent work, i.e., comparing rational (instrumental rationality) and an institutional model. According to the theory of instrumental rationality, given objective reality, complete knowledge, and unlimited mental processing capability, "institutions are unnecessary because markets are perfectly efficient" (Ibid., p. 3). In the contrasting institutional model, institutions are described as "rules of the game," and organizations, the players (Ibid.). In this conceptual economic system, it is the presence of institutions, not their absence, that enables greater market efficiency. However, while these broader economic concepts will present themselves in again in Chapter 10, works from the economics discipline were not the principal source for theoretical grounding of this dissertation.[44] Other distinguishing characteristics are discussed in the following sections,

---

[42] The term "natural system" refers to an organization as attending to its own maintenance and survival.

[43] Selznick (1996) stated that his work *Leadership in Administration* (1957) is "often cited as a source of the 'old' institutionalism in organization theory" (p. 270).

[44] Political scientists, economists, and sociologists have been writing about institutional attributes since the turn of the 20th century, and connecting their ideas to the structure and behavior of organizations since the 1940s. The interdisciplinary nature of the organization studies field has led to diversity in

where alternate perspectives on organizations are described: the rational system perspective in its classical and contingency forms, and the institutional system perspective.

A rational system perspective

> … [W]hat must be explained is an action, i.e., behavior that reflects purpose or intention. … [T]he action is chosen as a calculated solution to a strategic problem. … [The] explanation consists of showing what goal the [entity] was pursuing when it acted and how the action was a reasonable choice, given the … objective (Allison & Zelikow, 1999, p. 15).

The rational system perspective in organization theory has come to be associated with works by Weber ([1906-1924] 1946 / 1958), Taylor (1916), and various writers on "Fordism" principles (e.g., Sabel, 1982). Broadly, from a rationalist perspective, organizations are technical systems, referring to a way of organizing structures and activities "to lead to predetermined goals with maximum efficiency" (Scott, 1992, p.30).[45] The foundation of the model is the rational actor paradigm and its means-end process.

The rational actor paradigm is the process of ordering sets of preferences by a self-interested actor with complete knowledge and devoid of context or bias, with the goal of maximizing benefit. A rational model of organizing thus describes an identification, consideration, and ordering process of determining the best means toward a desired objective, and the organizing of work systems as a rational design process—the ordering of processes to facilitate efficiency in production, communication, performance

---

conceptions. This study is focused on those conceptions represented in the sociological literature. The term "institutional system perspective" encompasses ideas of both "old" and "new" institutionalism.

[45] In the review of information security literature, the term "technical" is used in connection with computer hardware and software. This term has an extended meaning in its use in organization theory.

monitoring, and decision-making. Employing a rational system perspective, an organization is a rationalized system linking means to ends.

Classical theory

Works early in the twentieth century from engineering, academia, and management (Taylor, 1916; Gulick & Urwick, 1937; Weber, [1906-1924] 1946 / 1958) employed rationalist concepts to organize the components of work systems in the best way for efficient production. Classical rationalists viewed an organization as a technical system, explicitly goal oriented and optimized for task performance within a closed system.

Works by sociologist Max Weber have had a profound influence on the concept of a rationalized system. Weber (1970) drew attention to bureaucratic forms of organization and their support for rational decision-making and administrative efficiency. This work portrayed an "ideal" bureaucracy as an elaborated work system that divides tasks into specialized segments for efficiently performing the activities of the organization.[46] The bureaucratic system defines work requirements for each position within a segment, and organizes the positions in a hierarchy of authority that provides both control and channels of communication. In this system, formally trained employees, using standard technical procedures and behavioral rules for their work, are rewarded based on competence. The bureaucratic model, with its simple rational design, is particularly evident in public organizations, and has become the dominant form of organization generally.

[46] Adam Smith ([1776] 1996) described this in his writing on the "division of labor."

Works by engineer Frederick W. Taylor, who represents the extreme in a rationalist perspective and well known for his development of methods for "scientific management," defined the organization of work systems using a bottom up approach. A work system included the objective of the job, the sequence of operations required to perform the job in terms of time and motion, and the standards for performance of the job. Taylor believed that by analyzing the job, managers could determine the optimal method for performing the job and therefore "standardize" the requirements, making production rationalized and predictable. His pioneering efforts contributed the concepts of objective and of standards (i.e., the ideal performance requirements for accomplishing an objective), and left a legacy in better understanding of how to produce efficiently and eliminate uncertainty. Taylor's ideas can be seen in the concept of a "best practice"—the idea of an industry standard for the best way to perform a particular business activity.[47] This idea is in keeping with Taylor's concept of a work system that included a human contribution only in the sense of finding the most skilled person to do the job, and providing adequate wages for its performance. He considered human behavior as simply a replaceable mechanism, a component of the work system, and organizations, if well structured, as efficient technical instruments for attaining a desired goal. Taylor's model provided a causal relationship between organizational actions (X) and organizational consequences or outputs (Y).[48]

---

[47] However, in contrast to Taylor's ideas of quantitative measurement and rational choice, the concept of an industry best practice, as discussed later, is an ephemeral description diffused within institutionalized environments.

[48] "Organizations are to be explained by scientific laws in which the shape taken by organizations is determined by material factors" (Donaldson, 1996).

As another example of rationalist ideas, Henry Ford is known for conceiving and implementing the production line, a way of organizing a manufacturing process that divides activities into very small elements. By using a highly specialized division of labor, his process (now called Fordism principles) introduced greater efficiency into the manufacturing of automobiles.

Management scholars' (e.g., Lyndall Urwick, and Luther Gulick) work carried the similar instrumental, rationalist objective of improving productivity, but as a top down approach across the entire organization, as opposed to the work of Taylor and Ford. The work of these scholars viewed the overall organization with the intent of enhancing effectiveness ("administrative management"), and emphasized the importance of structure as an influence on organizational performance.[49] Together with the efficient use of organizational resources, the implementation of management principles—clear definition of worker specialization, superior-subordinate relationships, roles within organizational hierarchies—predicted efficient organizations (Meier & Bohte, 2000).

Contingency theory

The contingency model is associated with works such as Donaldson (2001), Galbraith (1973), Lawrence and Lorsch (1967), Thompson (1967), and Woodward (1970). Like the classical theory, contingency theory has focused on technical organizational structure, but has offered a more complex model than the earlier view. Rather than closed systems this model describes organizations as open systems, which means, "affected by and affecting the environments in which they exist" (Scott, 1995, p.

[49] Structure as it is used here refers to the internal mechanisms supporting organizational activities—the division of labor and the coordination mechanisms for achieving the total objectives of the organization (Lorsch, 1970).

xiii). In addition, the model expands the classical view by recognizing that differences exist among organizations. Rather than a search for the one best way to structure and manage, contingency theory suggests not simple, but conditional, relationships between the characteristics of an organization and the performance of its specialized tasks in a dynamic and distinctive environment.

> … [T]he rational-contingency model views organizational actions as the result of choices made among a set of goals in an environmental context of constraints and opportunities (Drazin & Van de Ven, cited in Hall, 1996, p. 295).

Besides structural arrangements, a number of other variables, e.g., "individual, social, and organizational inputs," influence organizational outputs (Pennings, 1975, p. 1).

Contingency theorists claim that organizations adapt their internal functional structures in response to environmental changes. An organization focuses on its technical activities, shaping its work processes while protecting them from disturbances in the environment (Gupta, Dirsmith, & Fogarty, 1994).

> … [I]ndividual organizations adapt to contingencies and being in a state of adaptation means that the organization's structure 'fits' the contingency or contingencies that the organization is confronted with at a given point in time (McKinley & Mone, 2003, p.347).

Organization and Environment: Managing Differentiation and Integration (Lawrence & Lorsch, 1967) described one of the foundational studies of contingency theory. This study examined the structural design of organizations in various work environments: comparing manufacturing organizations that produced plastics with two groups of two others that produced containers and foods respectively. Evidence demonstrated that organizations create specialized sub-units to deal with various environments and that they adapt their internal structures to specific environmental conditions.

> Characteristics of the type of work being performed—the technology—and of the technical and institutional environment pose opportunities and challenges to which organizations respond (Scott, 1992, p. 124).

Consider an organization singularly focused on commercial air transportation. Passengers pay to be safely transported from a point of origin to a final destination. Within this organizational system, distinct subsystems perform tasks that must be integrated in order to accomplish this mission. Scheduling flights, interpreting air traffic and environmental conditions, ticketing passengers, screening and storing baggage, managing pilots, flight attendants, and other human resources are some of the myriad duties of functional subsystems.

A number of studies have examined work characteristics at the sub-unit level. The Lawrence and Lorsch study focused on a characteristic they called "task uncertainty" and found that sub-units performing predictable tasks (e.g., the production department) were more effective when they were formally structured, whereas sub-units performing tasks in an uncertain environment (e.g., the research and development department) needed a different structure. The sub-systems (sales, research, and production) in each organization were differentiated from each other in sub-system formal structures, as well as other attributes. The study concluded that differentiation was related to requirements of the sub-unit's particular sub-environment.

The Lawrence and Lorsch study provides a set of research findings and concepts that enable us to understand what characteristics an organization must have to be effective in a particular set of environmental circumstances. This study directs our attention to the environmental demands placed on the organization in terms of the degree

of differentiation, the pattern and degree of integration, integrative mechanisms, and conflict management behaviors (Dalton, Lawrence, & Lorsch, 1970, p. 12).

The Van de Ven and Delbecq (1974) study determined that "task difficulty" and "task variability" affected sub-unit structures. Becerra-Fernandez and Sabherwal (2001) examined "task domain" and "task variability" to determine the knowledge management processes required for performing sub-unit tasks.

Organizations in Action (Thompson, 1967) also directed attention to the importance of organization-environment adaptation. Different from Lawrence and Lorsch and others, the work focused on tying different organization perspectives to different functional levels—technical, managerial, and institutional (Parsons, cited in Thompson, p. 10)—that are more or less open to environmental pressures. Thompson proposed that a classical model would be suitable for describing the technical level, a natural system model for the managerial level, and an open system model for the institutional level. For Thompson, an organization can function as a rational, technical system by selectively compartmentalizing critical parts of organizational structure (Scott, 1992). The concept of uncertainty was viewed as central to organization theories: "Uncertainty appears as the fundamental problem for complex organizations, and coping with uncertainty, as the essence of the administrative process" (p. 159).

In later work, Gresov (1989) included the idea that organizational structures are socially constructed and may become institutionalized, and that certain practices may be symbolic as opposed to instrumental—ideas represented by the institutional model.

Contingency theory contains both similarities and differences when compared to the classical model. The most obvious similarity is that each contains the concept of a

goal. Further, each views an organization as a neutral technical instrument. Each seeks optimal performance under specific conditions. However, contingency theory provides a more complex description of organization that accommodates varying contexts of work systems. This theory seeks no one best way for designing an organization, because each organization has a different set of characteristics and environmental circumstances in which different sets of activities must take place. "The best way to organize depends on the nature of the environment to which the organization relates" (Scott, 1992, p. 89). The "model is complicated as soon as we move to a complex, multi-unit organization in which each unit strives to cope with a different part of the environment" (Lawrence & Lorsch, 1967, p. 209).

Limitations of the rational system perspective

Many works have described limitations in conceptualizing organizations as purely rational: the rational actor model with its goal paradigm, its bureaucratic structuring, and lack of consideration for institutional context. The rational actor, preference-ordering concept is limited caused by both cognitive and contextual constraints on the actor. March and Simon (1958) recognized these limitations in explaining organizational decision-making, one of the key components in efficient production activity. The work stated that because organizations operate in environments with endemic uncertainty and complexity, and human rationality is limited, decision-making is less than optimal. Simon (1976) argued that managers do not attempt to optimize organizational performance—the clear goal in the rational actor model—because of limited time and limited knowledge. Managers tend to "satisfice," or choose the first alternative that meets their minimum criteria. Simon argued that if managers really attempted to be completely rational and

comprehensive in their approach to organizational design, they would not have the capital and information resources to deal with more than a few problems at a time.[50] Problems that are handled are resolved with limited or uncertain information.

Taylor (2001) asserted that the rational model is incomplete as a theory of organization, especially in its description of the cognitive process. The model assumes a single decision maker, rather than the multiple actors involved in organizational decision-making.

> [I]nteractively produced intelligence is distributed, rather than located in a single brain. Because it is distributed, rather than linear, it is a form of reasoning that is at variance with the logical algorithms of traditional rationality. … [I]f rationality is distributed, reasoning must be the accomplishment of several individuals working in concert. Teams develop knowledge that is not simply the sum of the members' cognitive processes (p. 142).

Further, the idea of conflicts of interest is contrary to the foundational premise of a self-interested actor. Resolution of conflicts must occur in markets since other mechanisms—"power and influence processes, kinship and shared group membership, or even moral or ideological principles," are argued to be less efficient for resolving conflicting claims made by self-interested actors (Ferraro, Pfeffer, & Sutton, 2005, p. 11).

Goals are also problematic. If there are multiple and conflicting goals, a condition clearly identifiable in a complex organization representing multiple interest groups, how does a rational model of organization work? Empirical analyses have found that organizational goals are often "vague, contradictory, or multiple, with no clear indication of their respective priorities …" (Georgiou, 1973, p. 293). As evidence of this confusion, a considerable gap often exists between organization goals and the results of organization

[50] Cohen, March, and Olsen (1972) wrote about the many limitations on utility maximizing behavior within a given context, describing a "garbage can model" that incorporates complexities that inhibit rationality.

actions (Merton [1940] 1957/1968). The actual activities of organizations often center around the proper functioning of procedures, rather than on achievement of goals. Merton "emphasized the 'unintended consequences of purposive action,' and his junior colleagues [Selznick, Blau, Gouldner], who carried out early definitive studies of public and private organizations, each gave his own twist to the dual nature of organization" (Scott, 2004, p.3). "This phenomenon of goal displacement [i.e., where organizational outcomes are different from stated objectives] is perhaps the most frequently noted pathological aspect of large-scale organizations" (Sills, 1970). Hall (1996) suggested that official goals tell us little about the organization. More important are the "operative goals," those focused around the allocation of resources toward organizational functions, given the constraints on the decision making. Internal and external forces can influence operative goals and can deflect the organization significantly from its original purposes. Georgiou (1973) suggested, "Commitment to a goal paradigm has retarded analysis by requiring the disassociation of conceptual scheme from incompatible empirical findings on organizations" (p. 291).[51]

What about the design of bureaucratic structures? The elements of classical theory have serious shortcomings when applied to a complex organization, such as the challenges in coordination of work among multiple levels (Lorsch, 1970, p. 2.).

> Both the [classical] … and contingency approaches presume that [organizational] designs are planned, that criteria exist by which good designs can be distinguished from bad designs in terms of how the structures operate, and that designs meeting these criteria contribute to organizational performance (Pfeffer & Salancik, 1977, p. 17).

[51] Georgiou described the generalized understanding of organizations as "goal attaining instruments" as "an overwhelmingly accepted conceptualization" (p. 291). This conception thus may be called a paradigm as opposed to a theory or model.

Studies confirm the idea that "organizations are essentially rational, structurally speaking, but in dealing with an uncertain, unpredictable world, organizations necessarily fall short of the ideal" (Taylor, 2001, p. 141).

Classical works established a causal relation between organizational actions (X) and organizational consequences or outputs (Y), but did not go far enough to consider factors that complicate actions or other factors that ultimately shape organizational outputs. Work that is more recent leads us to understand the causal relationship as a contingent relationship. However, Schoonhoven (1981) and others (e.g., Drazin & Van de Ven, 1985; McKinley & Mone, 2003) have criticized contingency theory and studies that employ it citing unclear theoretical statements, and poor description of functional relationships.

[T]raditional versions of contingency theory … underrepresent the complexity of relations between technological uncertainty, structure, and organizational effectiveness" (p. 369). Contingency theory also falls short as an organizational model by "ignor[ing] … political considerations … (Hall, 1996, p 294). A rational model, representing a reductionist perspective, "dispenses with the need to engage with history, context, values, and conflict" (Reed, 2003, p. 294).

In many works that noted the limitations of a purely rational system model—a model that assigns dominance to the material forces that shape organizations and to the concept of eliminating uncertainty—the institutional system perspective became the focus. The next section presents a brief review of literature concerned with this complex and often confusing view of organizations, the second major perspective of interest to this dissertation.

An institutional system perspective

An institutional system perspective is associated with works such as DiMaggio and Powell (1983), Merton ([1940] 1968), Meyer and Rowan (1977), Scott (2001), Scott and Meyer (1983), Selznick ([1949] 1984), and Zucker (1987). These works describe an institutional system perspective as a natural, "open system" view of organizations that "highlights the importance of the wider social and cultural environment as the ground in which organizations are rooted" (Scott, 1995, p. xii). Research has shown that "organizational environments are not only technical, providing resources and information in support of the production of goods and services and rewarding efficient performance, but increasingly institutional" (Greening & Gray, 1994, p. 470), reflecting socially-constructed contexts with their associated constraints and incentives, and, reflecting practices that may defy rational logic. Thus, organizational behavior is bounded both by resource dependencies and by expectations of "acceptable," "reasonable," or "legitimate" behavior.

> Organizations compete not just for resources and customers, but for political power and institutional legitimacy, for social as well as economic fitness (DiMaggio & Powell, 1991, p. 66).

From an institutionalist perspective, organizations' "output goals … are often undermined or distorted by energies devoted to the pursuit of system goals, chief among which is the concern to survive" (Scott, 1992, p. 73).

In the case of complex, large-scale organizing and rapidly changing technologies, it is difficult to conceptualize an organization as the idealized, predictable system defined by the rational model. So much of the environment is uncertain and thus by definition *un*predictable that it has been more appealing for some researchers to investigate why

organizational purposes were not achieved—in contrast to pursuing the expectations of a rational model. According to DiMaggio and Powell (1991) and others (e.g. Cohen, March & Olsen, 1972; Perrow, 1984; Sagan, 1993; Vaughan, 1999), organizations are sources of both order and disorder.

> Thus, although we stress that rules and routines bring order and minimize uncertainty, we must add that the creation and implementation of institutional arrangements are rife with conflict, contradiction, and ambiguity (p. 28).

From an institutional system perspective, the behavior of an organization is neither simply an internally directed nor an externally determined rational system. In fact, components of institutional theory may well be described as the "residue" of rational theory, all of the possible non-rational explanations for organization performance. Thus, one of the daunting issues of the institutional system perspective is its multifaceted character. "… [I]t is often easier to gain agreement about what [institutional theory] is *not* than about what it is" (DiMaggio & Powell, 1991, p. 1). Further, that the terms "institution" and "institutional" encompass divergent perspectives has made it difficult to pin down a good description of the theory.

However, at this point it is useful to provide definitions of terms as a starting point. The following are definitions of "institutions":

> Institutions are symbolic and behavioral systems containing representational, constitutive, and normative rules together with regulatory mechanisms that define a common meaning system and give rise to distinctive actors and action routines (Scott & Meyer, 1994, p. 68).

> Institutions consist of cognitive, normative, and regulative structures and activities that provide stability and meaning to social behavior. Institutions are transported by various carriers—cultures, structures, and routines—and they operate at multiple levels of jurisdiction (Scott, 1995, p. xiii).

> Institutions are social structures that have attained a high degree of resilience (Scott, 2001, p. 48).

Restating the above in brief form, institutions are products of social interaction. Institutions regulate social interaction. In addition to rules and regulations, institutions include behavioral norms and established habits of thought.[52] Institutions transmit and support societal structures. Institutions affect organizations. Organizations can *be* institutions.

Now, if that isn't confusing enough, to provide meaning for the term "institutional," Zucker (1987) presented two defining elements,

1. a rule-like, social fact quality of an organized pattern of action (exterior), and
2. an embedding in formal structures, such as formal aspects of organizations that are not tied to particular actors or situations (nonpersonal/objective) (p. 444)

and three defining processes (DiMaggio & Powell, 1983, p. 150),

(a) imitative or mimetic, adopting successful elements of other organizations when uncertain about alternatives,

(b) normative, transmission of social facts generally from external sources such as the professions.

(c) coercive, pressure by other organizations—by cultural expectations and/or the state.

The coercive process "is central to state legitimation in the *environment-as-institution approach*…" (Zucker, 1987, p. 444).[53]

These definitions offer evidence that this theoretical space is fundamentally difficult to navigate. To aid the reader, in the next section provides insight into the meanings of some of the above concepts.

---

[52] Behavioral norms are customary principles and values used to make decisions—to assess or justify actions. These principles vary depending on the social system that maintains them.

[53] Zucker identifies two approaches in institutional theory: organization-as-institution, and environment-as-institution.

Concepts in institutional theory

The introduction to the section on theories of organization stated that employing a theory can help to relate causal mechanisms to *Y2K solutions*. Theories of organization can explain the *Y2K* solutions of Delta's functional business areas; and, explanation can have an impact on how information security is managed in the future. Fundamental to the use of theory is the understanding the meaning of concepts that comprise the theory. The above definitions for the terms institution and institutional employ concepts of institutional theory that have been developed over a long time and through a number of works. The purpose of this section is to highlight those concepts that relate to the present investigation in order to begin to understand the institutionalized contexts—therefore, the actions—of Delta's functional business area organizations. Toward this end, two important concepts are emphasized:

1. Institutions are socially-constructed symbolic structures.
2. In order to understand actions, the symbolic structure in which the action occurred must be taken into account.

The first concept is the idea that institutions are symbolic structures. The work of sociologist Emile Durkheim ([1901] 1950) described symbolic structures—shared structures of knowledge, belief, and moral authority, which, for Durkheim, were "social institutions" (Scott, 2004, p. 13). Ideas included that of "social facts," symbolic structures that are products of human interaction but are experienced as objective. Durkheim wrote that we "institute" external structures and behaviors that were initially in the subjective sphere of individual interaction (Alexander cited in Scott, 2004, p. 13). Behaviors then are *normative* institutional behaviors if they are

> … guided not primarily by self-interest and expedience, but by an awareness of one's role in a social situation and a concern to behave appropriately, in accordance with others' expectations and internalized standards of conduct (Scott, 1995, p. xv).

Such behaviors are "instituted" by culture—ritual behaviors, values, and belief systems, which affects strategic choice, technical performance mechanisms, and organizational outputs.

The second concept is that in order to understand action, the symbolic system in which it occurred must be taken into account. Weber ([1924] 1968) understood action as a response shaped by interpretation within a particular context, not based on mechanical stimuli. "Environmental stimuli must be cognitively processed by actors—interpreted by individuals employing socially constructed symbol systems—before they can respond by taking action" (Scott, 1995, p. xiii). Therefore, according to institutional theory, one must investigate social context and associated common meaning systems in order to understand an action.

> … [I]nstitutional logics constitute the cosmology within which means are meaningful, where means-ends couplets are thought appropriate and become the naturalized, unthought conditions of social action … (Friedland, cited in Lounsbury & Ventresca, 2003, p. 465).

In the above quotation, "means" is a technical concept that refers to the instrument, method, or mechanism for accomplishing an objective. "Meaningfulness" is an institutional concept, a shared understanding among members of a culture or society. As an example, according to a reporter, upon arrival in the Sentinel Islands to deliver aid following the December 2004 tsunami, an Indian coastguard helicopter was "attacked by tribesmen using bows and arrows" (Charles, 2005).[54] What did the islanders think was happening? How are we to understand their actions? One interpretation—the one the

[54] These islands in SE Asia are home to extremely isolated tribes.

reporter employed—is that they were threatened by the helicopters, and therefore, they were trying to defend themselves against what they perceived as an attack. According to this interpretation, the tribesmen employed the bows and arrows as *means* of protection. In contrast to the primitive weapons of tribesmen, industrialized nations understand means of protection as highly rationalized and computer-based weaponry. In these dissimilar cultural settings, the different defense mechanisms are their respective "naturalized, unthought conditions of social action," a common understanding of what means are best to enable a desired "end"—protection from enemies. However, another interpretation of the islanders' actions is that they were confused by the arrival of the helicopters. A volley of arrows signified a need for a helicopter to identify itself and state its mission. The islanders employed the bows and arrows as a *means* of communication. The point is, "[t]o understand or explain any action, the analyst must take into account not only the objective conditions but also the actor's subjective interpretation of them" (Scott, 2001, p. 57). In fact, regardless of the true explanation in this situation, if the particular action were simply "the way things are usually done," this suggests that *cognitive* processes operating for the most part beneath the level of consciousness dictated the action.

The rest of this section concerns the concept of institutionalization, and the idea that institutionalization distorts a rationalist view of decision making. Institutionalization attaches both the cognitive aspect described above and a temporal quality to social action. "… [I]nstitutionalization is both a condition and a process: Regulations, norms, and cognitive systems do not appear instantaneously but develop over time …" (Scott, 1995, p. xx). Over time, organizations tend to perform according to established routines, and for

their own preservation instead of according to a model of goal-orientation. According to Meyer, Boli, and Thomas (1994),

> Institutionalization … is the process by which a given set of units and a pattern of activities come to be normatively and cognitively held in place, and practically taken for granted as lawful (whether as a matter of formal law, custom, or knowledge) (p. 10).

Selznick (1996) described institutionalization as "infusion with value beyond the technical requirements of the task at hand" (p. 271).

Zucker (1987) stated that institutions, once established in a society, endure "even though they are collectively suboptimal" (DiMaggio & Powell, 1991, p. 4). Thus, Zucker noted that institutionalization places limitations on the process of rational choice. Institutions become embedded as "social facts," and therefore, organizations often cannot access the full extent of their options. These confusing concepts are implicit in an understanding of organizations as "embedded" in social contexts. Even though many aspects of organizing are the result of rational decisions, these decisions are embedded in an institutional environment, i.e., within symbolic and behavioral structures that define common ways of thinking and doing—sometimes channeling decisions and actions out of the reach of maximizing performance. An institutional model attempts to characterize the context within which a rationalized, technical system of organization must function.

In an institutionalized environment, decision alternatives not only become limited and obscured, but also decisions are not the result of a purely rational evaluation of alternatives and their consequences. "This logic of consequences can be contrasted with a logic of appropriateness by which actions are matched to situations by means of rules organized into identities" (March, 1994, p. 57). Organizations have identities; e.g., Delta is a transportation organization and therefore, has rules associated with that identity. For Delta to be a "legitimate" transportation organization, it must organize and perform in a

particular way. March and Simon described "organizational behavior as … rule following more than the calculation of consequences" (DiMaggio & Powell, 1991, p. 19).

Administrative Behavior (Simon, [1945] 1976) described how organizations work to simplify and support decision making in organizations (Scott, 2001, p. 27). Behavior is rational *because* choices are constrained and organizations are guided by rules. Value assumptions, cognitive frames, rules, and routines predetermine the preferences of individuals and enable "rational" choice. "Institutions do not just constrain options; they establish the very criteria by which people discover their preferences" (DiMaggio & Powell, 1991, p. 11). *A Primer on Decision Making* (March, 1994) described both the logic of rationality—in its ideal and its bounded versions—as well as the logic of appropriateness as "reasoned" behavior. Kingsley has summarized the two logics:

> The difference between the two is often summarized in the following phrase: under rational models, preferences drive decisions which drive actions, but under institutional models actions drive preferences which drive decisions (G. Kingsley, "Re: 10 page research project overview attached," E-mail to the author, 2005).

Framing the concepts

As discussed in the prior sections, institutionalists have introduced a number of concepts in the attempt to make sense of organizational actions that did not seem to fit a rational model. Since the concepts themselves are often complex abstractions and the theoretical contributions sometimes conflicting, organizing frameworks have been constructed in order to relate these concepts and themes (e.g., DiMaggio & Powell, 1991; Hirsch & Lounsbury, 1997; Scott, 2001; Zucker, 1987). Two frameworks have highlighted contrasting themes. In the first framework, "organization as institution" is contrasted with "environment as institution." In the second framework, "old institutionalism" is contrasted with "new institutionalism."

In the first framework, Zucker (1987) described two distinct theoretical approaches to the study of institutions and institutional effects:

> … Environment as institution assumes that the basic process is reproduction or copying of system-wide (or sector-wide…) social facts on the organizational level, while organization as institution assumes that the central process is generation (meaning creation of new cultural elements) at the organization level (p. 444).

Put into Zucker's framework, this dissertation adopts the first theoretical approach—*environment as institution*, and its process of reproducing sector-wide social facts onto the organization.

Next, DiMaggio and Powell (1991) framed institutional theory by pointing to limitations of the classical model, and advocating a "new institutionalism." Classical ("old institutionalism") works were for the most part in the camp of Zucker's second theoretical approach, *organization as institution*. Under this classical model, institutions are designed for legitimate and explicit social cooperation, coordination, and control. Institutions are socially-constructed agents (e.g., regulatory agencies). "Institutions are staffed and are created to do the job of regulating organizations" (Stinchcombe, 1997, p. 1). People create institutions in legislative bodies and international conventions. Institutions influence individual organizations, which may choose or decide whether to respond to institutions and how to respond, sometimes in the face of conflicts or, differing attitudes. Under this view, organizations must negotiate with their environments for resources and legitimacy, which emphasizes the capacity of organizations to construct and enact their environments. Acknowledging the influence of norms and values, theorists focused on dynamics, change, social construction, and intentionality, notwithstanding sometimes unanticipated consequences (Hirsch & Lounsbury, 1997, p. 407).

DiMaggio and Powell's "new institutionalism" portrayed institutions as structural constraints, and for the most part in the camp of Zucker's first theoretical approach, *environment as institution*. In this view, institutions *determine* organizational structures and practices. They "are implemented by diffusion, are exterior and constraining without exterior people doing the creation or the constraining" (Stinchcombe, 1997, p. 2). In addition to rules and regulations, which are explicit, institutions can be subtle—like social habits or performance patterns. Institutional theorists in this second camp thus have rejected intentionality, and have stressed instead the routine nature of most human behavior. The preferences of rational actors are seen as constituted by institutions. Theorists have focused on "statics, outcomes, cognition, and the dominance and continuity of the environment" (Hirsch & Lounsbury, p. 407) to which organizations conform to achieve legitimacy. This dissertation adopts the new institutionalism approach, positing that organizational decisions are primarily influenced by institutionalized environments, which provide the best possibility for survival as opposed to that of efficient operations.

Considering the contrasting views of institutions, institutional conformance may be envisioned as spanning a spectrum of two extremes: At one end, conformance is among conscious alternatives in the act of ordering preferences in an organization. At the other extreme, conformance action takes place completely without reflection. Some have advocated integration of sociological theories into a single model, "the analysis of the experience of social agents and the analysis of the objective structures that make this experience possible" (Bourdieu, quoted in Camic & Gross, 1998, p. 456).

In Scott's opinion, "the most consequential dispute [existing among variations of institutional theory] centers on which institutional elements [normative, regulative, and cognitive] are accorded priority" (p. 50). Normative and regulative elements are interconnected and mutually reinforcing. Normative consensus creates an understanding of what constitutes acceptable or legitimate activity. Even social theories can create norms. Ferraro, Pfeffer, and Sutton (2005) described

> how the dominant assumptions, language, and ideas of economics can exercise a subtle but powerful influence on behavior, including behavior in organizations, through the formation of beliefs and norms about behavior that affect what people do and how they design institutions and management practices (p. 20).

Regulative elements constrain, channel or direct organizational activities by establishing rules, and associated monitoring or enforcement mechanisms. "A stable system of rules, either formal or informal, backed by surveillance and sanctioning power, is one prevailing view of institutions" (Ibid., p. 54). Although regulative elements can benefit prejudiced arrangements, e.g., vested interests, they also support the prevailing norms of a society. Cognitive aspects come into play in the concept of embeddedness. Such aspects as routines, rule following rather than rational decision making, etc lie in this category. A focus on legitimacy is paramount.

DiMaggio and Powell (1991) stated that, within all of these attempts at characterization, the whole point of institutional analysis is "to develop robust explanations of the ways in which institutions incorporate historical experiences into their rule and organizing logics" (p. 33).

Institutional effects in organizational fields

The discussion now turns to the application of institutional concepts at the level of organizational fields, which relates to the analysis of this dissertation. The paragraphs

that follow provide definitions for institution, institutional, and institutionalization; and, frame some of the concepts that have been incorporated into the institutional system perspective. Recall that institutional theory relates institutionalized aspects of environments to organization actions. Institutionalized aspects of Delta's business area environments contributed to its *Y2K solutions*. The purpose of this section is to demonstrate how the institutional system model has incorporated another environmental-level concept wherein groups of organizations, called organizational fields, exhibit similar characteristics.

This concept of organizational fields links organizational activities horizontally and vertically to "organizational structures and processes that are industrywide, national or international scope" (DiMaggio & Powell, 1991, p. 9).

> The visible structures and routines that make up organizations are direct reflections and effects of rules and structures built into (or institutionalized within) wider environments (Scott & Meyer, 1994, p. 2).

Scott and Meyer (1983) pointed out the great variety of wider environments identified as societal sectors, representing increasing numbers of significant vertical connections. Sectors vary in important respects, such as in their domination by either institutional or technical processes; and, the various sectoral characteristics are expected to influence strongly the number and types as well as the structure and performance of organizations within each sector. Thus, e.g., "regulatory processes may be expected to assume quite different guises and to have different effects in the medical care sector than in the civil aeronautics sector, reflecting not only differences in political processes [see Wilson, 1991] and economic mechanisms [see Knoll, 1971] but organizational arrangements" (p. 137).

While sectors or fields are different from each other, the similarity (i.e., homogeneity) among organizations within a field relates to the organizations' shared environment. Delta's business areas are elements of wider environments, and studies have demonstrated that wider environments have a homogenizing effect on internal organization activities among groups of organizations in the same field.

> The concept that best captures the process of homogenization is 'isomorphism.'... [I]somorphism is a constraining process that forces one unit in a population to resemble other units that face the same set of environmental conditions (DiMaggio & Powell, 1983, p. 149).

Related groups of organizations often display isomorphism in their homogeny of structures and processes when viewed from a broader perspective. Among organizations exhibiting isomorphism, similar internal functional structures have diffused and replicated over time as they responded to issues of competition and other external changes, and a focus on the appearance of legitimacy.

Legitimacy signifies looking like and performing like an organization that claims a stated purpose. Institutionalists have shown that organizations adopt organizational models that are accepted as appropriate for organizations populating the particular field to which they belong. The idea is that organizations depend on external support for survival; therefore, they comply with social expectations, laws, and regulations in order to maintain legitimacy and desired public image, but otherwise separate their internal technical activities from public scrutiny.

A consensus credits ideas concerning legitimacy to two articles as foundational works: (1) Meyer and Rowan (1977), "Institutional Organizations: Formal Structure as Myth and Ceremony"; and (2) DiMaggio and Powell (1983), "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields." Meyer

and Rowan's article is associated with the concept of symbolic vs. instrumental behavior. That is, organizations outwardly demonstrate institutional conformity, i.e., maintain a status of legitimacy using symbolic means in order to pursue appropriately their own technical purposes.

DiMaggio and Powell's article described the idea of isomorphism among organizations in a field, which is associated with actions that support legitimacy. Within common cultural frames such as exist in an organizational field, industry sector, or society, institutional influence actually comes more through "the diffusion of standard rules and structures … than the adaptive custom-fitting of particular organizations to specific settings" (Ibid., p. 27). The article discussed how the powerful organizations in a field exert pressure for conformity on others. The influence of power structures and vested interests has an important role in developing and maintaining norms and regulations.

Some institutional sectors or fields contain environmental agents that are sufficiently powerful to impose [or authorize] structural forms and/or practices on subordinate organizational units (Scott, 1987, p. 501).

Receiving a stamp of legitimacy by such agencies may be tantamount to survival for an organization. According to Astley and Van de Ven (1983), institutions

> embody a response to vested interests residing in their environments … Political domination, rather than technical efficiency, is held to underlie the design of organizational structure … The political domination argument thus requires that we shift our analytical focus away from the organization, toward broad social dynamics that unfold at a collective level of analysis (p. 264).

At this "collective level of analysis," a set of agents—e.g., industries, the state, professions—disseminate organizational models, which are adopted by organizations through the following three mechanisms: [55]

1. coercive isomorphism …, [which] stems from political influence and the problem of legitimacy;
2. mimetic isomorphism resulting from standard responses to uncertainty; and
3. normative isomorphism, associated with professionalization (DiMaggio & Powell, 1983, p.150).

Coercive isomorphism may come through legal and regulatory environments, where organizations in a particular field are subject to the same constraints and require organizing around those requirements. Mimetic behaviors derive from the historic look and feel of organizations that operate in a particular sector, and often arise in response to uncertainty. Mimetic isomorphism is also achieved by organizations sharing knowledge and strategies via consulting firms and professional alliances—environmental sources of influence that may encourage practices outside a purely instrumental model of behavior. Normative isomorphism occurs in order to demonstrate conformity with social and/or professional requirements in a competitive environment.

A number of works have examined these homogenizing mechanisms in field-level analyses. The paragraphs that follow provide brief summaries of the findings in five of these studies, in which institutional features that are particularly relevant to the approach in this dissertation are incorporated.

In the first study, Fligstein (1991) provided empirical evidence of the DiMaggio & Powell thesis regarding the mimetic process of isomorphism and its mechanism of diffusion in organizational fields in a study of the spread of diversification strategies

[55] Zucker (1987) identified these mechanisms as "defining institutional processes."

among U.S. corporations. The study showed that key actors in organizations who were in favor of diversification provided the momentum to adopt new strategies. Once influential organizations began to diversify, others began to imitate the new model. Fligstein showed that diversification "was a historically specific process that was shaped by the existence of organizational fields and the shocks provided to those fields over time" (p. 335).

Next, Galaskiewicz and Wasserman (1989) explored DiMaggio and Powell's thesis that under conditions of uncertainty organizational decision makers will mimic the behavior of other organizations in their environment, an idea related to the problem of decision making under conditions of incomplete information. Investments in boundary-spanning roles and strategic board members are examples of approaches to providing information that is more complete. The findings of this study show that networks are critical to mimetic processes.

In the third study of interest, Lounsbury (2001) sought to understand why responses to institutional pressures differ among organizations. While studies have focused on how organizational pressures for conformity weigh against technical demands of organizational activities, i.e., opposing forces that lead to practice diversity, "[t]here has been virtually no empirical research … directed toward understanding how variation in the content of organizational practice is systematically shaped by institutional forces" (p. 30). Findings showed that variation in staffing of recycling programs among educational institutions was shaped by a national social movement organization that provided resources and support to particular schools. These results suggest that "[a] focus on organizational heterogeneity can help to bridge the gap between institutional analysis

and more traditional perspectives of organizational adaptation that portray organizational variation as antithetical to institutional analysis" (p. 50).

In the fourth study, Mezias (1990) compared applied economic models and an institutional model in an empirical study of financial reporting practice at the Fortune 200 between 1962 and 1984, in order to understand the effect of changes in institutional frameworks on organizations at the field level. The study demonstrated how both changes in the field of federal agencies and the professional bodies responsible for setting accounting policy resulted in changes in the financial reporting practices of corporate organizations under their jurisdiction. The findings indicate that the institutional model adds significant explanatory power over and above rational models.

In the fifth study, Scott, Ruef, Mendel, and Caronna (2000) examined the variety of changes in organization of medical services in a single geographical area within a single industrial sector over a three year period. The study involved the examination of populations in three organizations, as well as the effects of changes in these populations on each other. Over the three year period, fundamental changes were experienced in the common understanding of how medical care should be delivered and financed, and who has the legitimate right to make such decisions.

These studies revealed homogenizing mechanisms in institutionalized environments in various sectors and settings. The studies also provided evidence that institutional analysis is important for understanding how changes at the field-level affect organizations, and for understanding organizational variation, all of which helped to guide the analysis of Delta's *Y2K solutions*.

Limitations of an institutional system perspective

Critics of institutional analysis have pointed out difficulties in defining the concepts and understanding how to resolve the issues of institutional theory. Disagreement exists on the basic assumptions and claims of the institutional system perspective. DiMaggio and Powell's advocacy of a new institutional system model was based on their idea that old institutionalism limits itself in its concern with internal and local organizational environments, while neglecting important wider environmental influences. Others (e.g., Greenwood & Hinings, 1996; Hirsch & Lounsbury, 1997) suggested that the models should be integrated to include both the old model's stronger agency perspective, and the new model's stronger structural perspective, and empirical evidence of this has been demonstrated (Arndt & Bigelow, 2000).

However, a major problem with the institutional system model is its potential requirement for tautological understanding. Such understanding is flawed in that variables have reciprocal definitions, i.e., chicken and egg priority problems. Critics suggest that identifying culture as the source of thinking and acting makes for a fuzzy causal model. To what in the multiple aspects and levels of culture can one attribute causation? Moreover, if the cause is embedded in culture, then what? Can culture be altered to achieve strategic objectives? Similarly, the term institutionalization is used in two conflicting ways:

> Institutionalization as an outcome places organizational structures and practices beyond the reach of interest and politics. By contrast, institutionalization as a process is profoundly political and reflects the relative power of organized interests and the actors who mobilize around them (DiMaggio, 1988, p. 13).

This suggests that a large number of organization situations and problems can be described as institutionally-based, and therefore de-emphasize the importance of a focus on efficiency.

Comparing the rational and institutional system perspectives

Rational and institutional system perspectives offer different and contrasting perspectives for understanding organizations. The rational perspective focuses on individual, autonomous organizations and strategies for efficient management, and emphasizes reducing uncertainty in order to achieve predictable organization performance. The classical form conceptualized organizations as closed technical systems that seek the one best way to organize in order to maximize productivity and reduce uncertainty. Early works focused on designing and standardizing work tasks, labor organization, and coordination mechanisms in order to achieve optimum performance toward a well-defined organizational goal.

Contingency theory is an elaboration of the rational, goal-based perspective, where the organization is conceived as an open system. Contingency theory claims that to understand the behavior of an organization requires more than examination of tasks as in the classical view; also required is consideration for the organization's environment. Important are logistics and task coordination structures that adapt to demands of changing environments. In a rational model, output reports can show results of process implementation and progress toward goals, whereas an institutional model must rely on interpretive examination to assess organizational functioning.

Institutional theory conceptualizes an organization as an open system where elements of its institutional environment affect the organization's technical performance

mechanisms and outputs. These elements include the concept of performance according to socially-constructed cultural influences and established routines. Theory represents organizations as focused on the maintenance of legitimacy instead of the rational model of goal-oriented efficiency. In a particular sector or society, organizations exhibit isomorphism created by the pressures of institutional environments, resource dependencies, and their competition.[56]

The institutional system perspective is focused on environmental influence at multiple levels of analysis. The concern is with social institutions rather than technical performance. Institutions include collective norms of acceptable behavior, settled habits of thought, organizations that display characteristics of institutionalization and political domination. Studies have sought understanding of institutional decision-making and have assumed unpredictability with respect to organizational outputs.

Integration of the two perspectives has been proposed (Scott, 1992, p. 96; Abell, 1995, p. 14) in order to provide a more complete picture of an organization's influences. One way of resolving conceptual inconsistencies is by the consideration that conforming to institutional expectations may be viewed as a rational act.[57]

Summary

An overview of literature in the information security field was presented in this chapter. Using the four-quadrant matrix developed in Chapter 1, the non-technical dimension was targeted for review, stating the discovery that most of the contributions to

[56] Recall that isomorphism refers to a process whereby organizational characteristics diffuse within a field to create more similar organizations over time (Scott, 1992, p. 209).

[57] Gupta, Dirsmith, and Fogerty (1994) claimed to be the first to integrate these two perspectives in analyzing an organization.

knowledge were confined to the activities within organizational boundaries, thus providing a rationale for research that employs sociological theories of organization. Next in order was a review of the literature on rational and institutional theories of organization, wherein the two perspectives were compared.

The empirical investigation proposed in this dissertation—an investigation of the influence of institutionalized environments on technical and procedural security approaches of organizations—fits within the non-technical-environment quadrant of information security studies, an area unexplored in information security research. This dissertation can help to fill a gap in our knowledge and can have broad implications. The new understanding can add insight that may help to answer the big question that will remain: *How can we design and implement security strategies that are both politically acceptable and technically effective?*

CHAPTER 3

SETTING UP THE INVESTIGATION

> Experience shows … that the social and political aspects of organizations appear to have a significant impact on the manner in which information technology systems are conceived, designed and implemented (Dhillon & Backhouse, 2001, p.133.)

This chapter presents a statement of the specific problem for investigation, and the structuring elements of the dissertation: the setting, hypotheses, and research design.

The research problem

- Information security management is complex. In an organization, it involves dealing with complex environments both inside and outside organization boundaries, and involves a combination of non-technical and technical issues.
- To manage the security of information and information systems effectively, an institutional infrastructure must be coordinated among organizational, social, and political systems.
- Research on technical components, i.e., hardware and software, has dominated the literature. Ways of envisioning and understanding the problem need creative expansion in the attempt to lessen the serious consequences of information security failures.

This dissertation fills a gap in the information security literature by focusing on institutionalized environments of organizations. The research examined the process of eliminating an information security problem in a complex organization. The focus of the investigation was the *Y2K* compliance solutions at Delta.[58] Guided by organization theory, the dissertation analyzed contextual conditions that affected the compliance process in Delta's sub-unit business areas. The focus of the investigation was on the ways in which institutionalized environments "complicate and constitute the paths by which

[58] Legislative action required Delta, like many organizations in the U.S., to pursue Y2K compliance and to provide evidence of their progress toward achieving success.

solutions are sought" (DiMaggio & Powell, 1991, p. 11). Neither the cause of the *Y2K* problem, nor the immense public interest in it was part of this work. Rather, the investigation concerned the effects of contexts within which Delta sub-unit business areas pursued solutions to their *Y2K* problems once this information security vulnerability was identified.[59] This dissertation demonstrated how knowledge about the institutionalized environment of an organization can reveal not only issues that compound and frustrate information security management, but also ways to enlist support.

Why study Y2K?

> Airline and transportation industry have the most dependency on automation and therefore have the biggest challenge for BCP [business continuity planning] (Gartner Group, 1999, cited in Delta archve, "Delta Year 2000 Program Briefing Book," 1999, p.5).
>
> The *Y2K* transition will occur worldwide (and even in space). … [W]e have little past experience with *Y2K*-like transitions (Neumann & McCullagh, 1999, p. 144).
>
> A simple explanation for the *Y2K* problem: The *Y2K* problem comes from the fact that people trust idiot savant computers with their lives (Cohen, 1998, p.9).

The technical description of *Y2K* was simple. A long-standing and widespread software coding practice, established to gain efficiency when computer memory was scarce, was to abbreviate the calendar year in the date code of computer programs. Such program code represented the year in a form that included only the last two digits: for example, the year 1968 was coded as 68. Although over the years, programmers acknowledged the computer date-coding scheme as a potential problem, this code endured for whatever reasons to cause an unforeseen global crisis, and the resulting lengthy and expensive process of repair and compliance.

---

[59] A distinction is made here between Delta sub-units and Delta subsidiaries, which are business areas that operate outside organizational boundaries.

The *Y2K* compliance process represented a coordinated effort both nationally and internationally to eliminate this small and specific detail from program code. In *Y2K*-flawed systems, which in the 1990s included many of the world's computer systems, the change to the year 2000 had unknown consequences. The functions of far-reaching networks were at risk; experts feared that airplanes would crash, financial systems would collapse, or other horrifying disasters would occur. The federal government's attempts to mitigate panic came with "no uniform definition of *Y2K* compliance, no uniform definition of testing, and little independent validation and verification" (Neumann & McCullagh, 1999, p. 144). Within a context of the ultimate danger to the nation, crisis decision making would ideally fall into a model of rational choice. In fact, the model Delta set out to follow in developing its Mission Possible: Year 2000 action plan was devised according to rational logic. However, this dissertation shows how Delta's institutionalized environment, coupled with the *Y2K* crisis, promoted institutional decisions and solutions that ultimately created information security risks.

Like all IT system vulnerabilities, the complexity of systems environments rendered the *Y2K* bug difficult to eliminate. Preserving the integrity of information was the essential concern. However, the digital date coding scheme ultimately affected all of the features of secure systems—the confidentiality of information, its availability, and its integrity; and all system functions—its authentication scheme, its content, its accessibility, and its operations. Therefore, the integrity of the data affected the control and safety of critical infrastructure systems. The *Y2K* problem thus provided an opportunity to examine a security vulnerability with all of the features and concerns of security problems that still exist in 2007.

However, different from examining a security problem of 2007, studying *Y2K* as a past issue offered logistical advantages. The event provided clear boundaries, both in time and in topic. It provided a clean beginning and ending point in time in terms of the *Y2K* event itself. In topic, the event provided a security problem for investigation that was in a stable environment, rather than the volatile environment in which information systems must function. The event also had a closed form, in the sense of project management. The problem solving process involved a beginning, middle, and end. Delta assembled a task force, developed strategies for addressing problems, prepared documents that recorded its progress, and implemented a variety of action plans to achieve success in solving its *Y2K*-related problems.

The setting: Delta Air Lines

Delta is a civil aviation enterprise that provides scheduled air transportation services for both cargo and the traveling public over national and international routes. A number of characteristics of the Delta organization made the setting well-suited for the focus and design of this dissertation.

First, it was a large organization with dispersed operations. By 1997, Delta had become the "most traveled airline in the world, carrying 101 million passengers."[60] For the fiscal year ending on June 30, 1997, passenger revenues accounted for 92% of Delta's operating revenues. Cargo revenue, which included freight and mail, accounted for 4% of Delta's operating revenues, and other sources accounted for the remaining 4%. Delta was the largest U.S. airline in terms of passengers carried, and the U.S. market leader in the world's two largest aviation markets, North America and the North Atlantic. With its

[60] Source for the statistics in this paragraph is Delta Air Lines (1997).

worldwide partners, Delta operated over 4,800 daily flights. Some 8,400 Delta pilots and 18,000 flight attendants formed flight crews serving on approximately 550 aircraft, and its total employees numbered over 63,000. Atlanta, Delta's headquarters since 1941, was the world's largest airline hub.

Second, Delta was a complex organization. The organization had also developed a complex environment, which may be characterized as simultaneously technical and institutional. See Table 3. As part of its technical environment, Delta had established a flight network that extended to 149 domestic cities in 42 states, as well as 41 cities in 25 foreign countries.[61] Because of its extensive reach and its long-standing political involvements, Delta's institutional environment included domestic and international regulatory agencies, unions, and other organizations in the air transportation industry in both U.S. and international spheres.

[61] These figures represent Delta's routes as of August 15, 1997. The complex route network included the Delta Shuttle, Delta Express, the Delta Connection program and the firm's alliances with foreign airlines.

Table 3: Delta's organization-environment complexity

ENTERPRISES

- Passenger services
  - Domestic & international
  - Delta Shuttle
  - Delta Express
- Freight operations
  - Delta DASH
- Information Technology services
  - Worldspan
  - *TransQuest/Delta Technology*
- Delta SkyMiles Program
  - Delta Loyalty Management Services, Inc
- Organization staffing services
  - Delta Staffing Services
- Communications services
  - DeltaTel

DOMESTIC AND INTERNATIONAL OPERATIONS

- Airports
- Delta Connection carriers
- Other airline relationships
  - Alliances
  - Code-share services

CONTINGENCIES

- Competitive market activities
  - Competitors
  - ACE Aviation
  - AirTran Holdings
  - Alaska Air Group
  - Amadeus
  - AMR Corp
  - British Airways
  - Cathay Pacific
  - Continental Airlines
  - Galileo Intl
  - Hawesko Holdings
  - JetBlue Airways
  - Japan Airlines
  - KLM
  - Lufthansa
  - Mesa Air
  - Northwest Airlines
  - Qantas
  - SAS
  - Sabre
  - Singapore Airlines
  - Southwest Airlines
  - TACA
  - UAL
  - US Airways
  - Virgin Atlantic Air
- Fuel availability and cost
- Scheduling
  - Airports
  - Maintenance
  - Partner airlines
  - Personnel
  - Weather
- Union activities

RESOURCE DEPENDENCIES

- Internal assets
  - Aircraft
  - Facilities
  - Computer-based systems (IT) [62]
    - Bag & mail sort systems
    - Finance functions
    - Flight training devices
    - TOC tools
- Customers
- Funding, financial operation
- Human resources
  - Skills
  - Certifications
  - Pay scale
  - Security clearances
- Personnel
  - Airport flight controllers
  - Pilots, flight attendants
  - Mechanics
  - IT workers
  - Other
- Critical suppliers
  - Fuel
  - Aircraft
  - Aircraft parts & tools
  - Food service

REGULATORY AGENCIES

- Government
  - APHIS, plants & health inspections
  - U.S. Customs
  - DOT, antitrust, int'l
  - EPA
  - FAA, safety
  - ICAO
  - INS, immigration
  - IRS, domestic & foreign taxation
  - NWS, weather
  - NavCanada
  - NOAA, ocean & atmosphere
  - OSHA, workplace safety & health
  - DOJ, security
- Industry-owned organizations
- Unions

CORPORATE COMPLIANCE RESPONSIBILITIES[63]

- Antitrust, embargoes and trade sanctions
- Copyright and other intellectual property
- Employee Retirement Income Security Act (ERISA)
- Environmental
- Falsifying company records, drug trafficking or use
- Federal contract procurement policies
- Finance Foreign Corrupt Practices Act and other anti-bribery and anti-kickback laws
- Immigration (including employment of aliens)
- Political activity
- Securities reporting and corporate governance

[62] IT systems perform information processing within all of the functional areas of the airline.

[63] This list is not intended to be all-inclusive ("Corporate compliance is everyone's responsibility," 1997, p.10).

Third, as a leading U.S. airline, Delta was also a critical organization. Civil aviation is the heart of the travel and tourism industry, which during this study period was the second largest U.S. economic sector.[64] Aviation and related industries were contributing $800 billion to the U.S. economy, or about 8% of the total GDP (Mullin, 2003). Thus, airlines could be considered critical sector organizations, not only because of the function they serve as facilitators of commerce and of civil and defense industries, but because they provided a significant portion of the economy.[65]

Fourth, to complicate its critical sector status, Delta was highly dependent on computer-based information systems to run the business. Inasmuch as the many business areas of this organization were required to work together to produce Delta's finished product, that of safe and reliable transportation, reliable and timely information was vital to their business operation. Indeed, flights were at risk if an IT malfunction impaired systems related to airline operations.

> Some of the most … widely used systems include those for air traffic control, navigation, reservations, and aircraft flight control. Others are used … for airport and airline management. … Neumann … believes many of these systems are poorly designed with respect to security and are at risk to GPS jamming, electromagnetic interference, denial of service, Trojan horses, disgruntled employees, and other threats (Goodman, 2001, p.70).

Goodman suggested that the transportation sector might serve as a useful example and precedent for other major sectors in dealing with the problems of information

---

[64] "The economic impact of aviation is so big it's almost beyond measure. Revenues generated by airports like Chicago O'Hare, Dallas/Fort Worth, and Hartsfield Atlanta run in the billions. … And as we were reminded so painfully after September 11, travel and tourism, which depends on the airlines, accounts for one out of seven jobs in America, and is among the top three employers in 29 states" (Garvey, 2002).

[65] "Hartsfield pumped $9.3 billion into metro Atlanta's economy in 1997 … according to an economic impact study released by the airport. The … business revenues, along with the creation of 9,771 new jobs … at the airport, make it vital to Atlanta's economy" (Hartsfield City Limits: A $9.3 billion a year impact, 1998, Nov 2).

security, especially with respect to cyber crime and terrorism. The reasons he cited related to civil aviation as not only "one of the most widespread and extensively interconnected international infrastructures" (Ibid.), but also that the enterprise has a long history of successful collaboration to resolve problems. Thus, it seemed valuable to understand how Delta dealt with the *Y2K* bug.

Finally, an important characteristic of the Delta organization with respect to this dissertation was the generosity with which its senior management accommodated the dissertation's development. Early in the dissertation design stage, Leo Mullin, who had served as Chairman and CEO of Delta during the years of the Year 2000 Program, arranged access to the Delta organization for purposes of this dissertation.[66] Through this connection, the extensive documentation of the Year 2000 Program in the form of CDs and printed documents was made available. In 2006, access was facilitated through the office of Gerald Grinstein, CEO and long-term Delta Board member.

In summary, Delta was appropriate as a target for this investigation because:

- Delta was as a large, complex organization, and characterized the differentiated environment within which security mechanisms must often be implemented. Further, the environment of the organization was simultaneously technical and institutional.
- Delta operated within a critical infrastructure sector.
- The organization's operations depended on the reliable functioning and trustworthiness of networked information systems. Scheduling (time, place, date) of operations was critical; therefore, Delta's ability to comply with the directives of *Y2K* policy was related to its ability to continue to deliver service and to the ultimate survival of the organization.
- The organization had detailed written documentation of the *Y2K* compliance process.
- Delta provided access to the organization and its archives for purposes of this work.
- The administration of the Year 2000 Program had been carried out in Atlanta; therefore, sources of information were convenient to the investigation.

[66] The author's first visit to Delta took place in January 2004. Mullin had resigned as CEO, which was effective in December 2003; but he had stayed on as Chairman through April 2004.

The Year 2000 Program

The goal of Delta's Year 2000 Program was twofold. First and foremost, the goal was to eliminate the *Y2K* vulnerability in all of Delta's computer-based information systems, and to verify the *Y2K* compliance of IT systems outside Delta's boundaries that affected its operations. Since these goals involved the entire organization, a process was devised that engaged all of Delta's business areas.

When *TransQuest* was started, Delta's IT staff had first sorted the IT systems into groups (i.e., Portfolios of systems) that supported the four core business areas. These technologies similarly formed the basis for the organizational divisions when *TransQuest* became *Delta Technology*.[67] The Year 2000 Program structures incorporated multiple parallel activities within these Portfolio divisions.

As described earlier, the Delta organization was a good target for investigation in a number of ways; but *convenient* aspects existed within the Year 2000 Program also—in addition to particularly *interesting* aspects, and some *puzzling* situations that motivated further inquiry. From a convenience standpoint, not only did the Delta Year 2000 Program serve to operationalize the concept of information security, but also it was well structured for analysis. In each business area, project activities pursued the same goal in an identical manner; but in each business area, these activities unfolded in a different context and resulted in different solutions. The evidence of different solutions among the parallel business areas allowed investigation of the influence of organizational and environmental contextual features.

---

[67] Delta Technology is Delta Air Lines' wholly owned subsidiary organization whose activities are dedicated to the development and support of Delta's information technologies. The *Delta Technology* portfolio divisions align with the Delta Air Lines functional business areas and are considered interchangeable units for purposes of this work.

Interesting and puzzling initially was the way the plan was carried out. In the process of trying to get the project underway, a secondary goal emerged. Along with the primary goal of eradicating the *Y2K* bug, this secondary goal, was to overhaul everything—to modernize and streamline the IT systems for better service to the needs of the organization. At first glance, the decision was puzzling. The goal seemed to run counter to the notion of eliminating security vulnerabilities; it appeared to be adding unnecessary complexity to an already risky situation. It seemed that the decision-makers must have been either painfully ignorant or incredibly courageous. Adding to the puzzle was the question: did all of this "tinkering" with a complex system that worked adequately before the project started invite problems as a result? Was it luck that Delta was overwhelmingly successful in achieving its goals? Prior theories would suggest that *something* had gone awry with this plan in such a large, complex organization. As it turned out, as this secondary goal was met it would both strengthen and weaken information security. Strength would come by standardizing hardware, replacing outdated systems, and by gaining a better general understanding of how the systems worked together. The weakness would come by standardizing systems and employing a common network protocol to connect them all, thereby opening the door to security problems.

Research hypotheses

As the characteristics of Delta's Year 2000 Program came into focus, the question emerged that served as the basis for the design of the investigation, i.e., *why the disparity among Y2K solutions of Delta business areas?* What caused the difference in compliance response? The investigation would resolve other questions while answering this central inquiry.

From a rational perspective, the answer to the question relates to the variation in task environments of the business areas. Business area structures and processes depend on the nature of the tasks that a business area performs (and the conditions in its IT systems); therefore, while pursuing the goal of the organization (i.e., removing the *Y2K* vulnerability, etc.), the task environment of each business area shaped its internal rational responses.[68]

From an institutional perspective, structures and processes in business areas depend on not only the nature of tasks and the associated IT systems, but also on conditions in their respective institutional environments. Therefore, the answer from an institutional perspective is that *Y2K* goals became secondary to institutional forces—regulative, cultural, and mimetic processes, and produced institutional responses that varied depending on the business area environment. The answer would suggest that *legitimacy* rather than efficiency was the ultimate driver for a Delta business area solution.

To test these propositions, this investigation considered competing hypotheses that reflected the institutional system and rational-contingency system perspectives, respectively:

Hypothesis 1: the institutional system model: *The Y2K solution in a Delta business area can be explained as an institutional response to contextual conditions, which is related to sector-based institutional mechanisms.*

Hypothesis 1a: A business area solution was an institutional response influenced by industry regulation.

---

[68] This means viewing each business area at the aggregate level based on the predominant nature of its tasks, while recognizing that each business area performs numerous tasks that are not all similar (Becerra-Fernandez & Sabherwal, 2001, p. 27).

Hypothesis 1b: A business area solution was an institutional response influenced by inter-organizational relationships.

Hypothesis 1c: A business area solution was an institutional response that imitated the solution of other organizations.

Hypothesis 2: the rational-contingency system model: *The Y2K solution in a Delta business area can be explained as a rational response to contextual conditions.*

Hypothesis 2a: A business area solution was a rational response to technical system conditions.

Hypothesis 2b: A business area solution was a rational response based on cost/benefit evaluations and availability of resources.

Consistent with the findings of Fligstein (1991), Galaskiewicz and Wasserman (1989), and other studies reviewed here, business area solutions associated with the Year 2000 process were predicted to conform to the first hypothesis: institutional responses demonstrating influences that stemmed from the institutionalized environments of their respective organizational fields.

Research design

> A research design is the logic that links the data to be collected … to the initial questions of a study (Yin, 1994, p.18).

The research was designed as a case study. The case study included analysis of four Delta business areas as embedded sub-cases: *Business Support*, *Airport Customer Service*, *Operations*, and *Revenue*, and their respective sub-environments; therefore, the unit of analysis was the business area-environment system. Their respective activities, resources, and sets of actors had differentiated these business areas from each other and had led to distinct IT systems that assisted their performance. The characteristics of these business areas also included somewhat distinct technologies and relationships in the organization-environment sub-systems within which each operated. The investigative

methodology included comparison of the four business areas with respect to three variable constructs: *Y2K solution*, *environmental context*, and *response assessment* (See Table 3). The study attempted to learn what conditions were influential in leading to individual business area solutions, and to assess the solutions as rational or institutional responses, based on institutional or rational-contingency theory concepts. Employing a comparative method, the investigation attempted to isolate any contextual conditions that the business areas shared in the attempt to reveal causal factors for their differences; and, attempted to determine which of the rival models better fit the organization actions.

The term "contextual conditions" or "*environmental context*" refers to conditions that existed within a business area-environment system—conditions relating to its task environment (which included its IT systems), and to its institutional (cultural and regulative) context. Assessment of a *Y2K solution* as rational or institutional (*response assessment*), with respect to the *environmental context* that influenced the *Y2K solution*, related to the performance expectations for a rational-contingency system model or an institutional system model, respectively.

Model variables

The dependent variable, *Y2K solution,* was defined as *changes to software systems in a functional business area of Delta over the period 1997-2003*.

An independent variable, *environmental context,* was defined as a set of conditions that existed in a business area-environment system that impinged on the decision processes. *Environmental context* had two components: *task environment* and *institutionalized environment*, the latter representing the cultural and regulative context of the business area. *Task environment* was operationally defined as functional activities and

supporting technologies; *institutionalized environment* comprised cultural context and "federations, associations, customer-supplier relationships, competitive relationships, and a social-legal apparatus defining and controlling the nature and limits of relationships" (Pfeffer et al., 1978)—structural systems that had become established over time.

A third variable, *response assessment*, related to the *Y2K solution*. *Response assessment* was a binary variable whose value was either "rational" or "institutional," relating to a *Y2K solution* as either predominately rational or predominately institutional in response to the *Y2K* mandate.

"Predominantly rational" was operationalized as the relative prominence of features or mechanisms that lead to a relatively more or less efficient or effective solution. These mechanisms, which are associated with a rational-contingency model of performance, are related to organization of labor, goal orientation, attention to efficiency of operation (reducing complexity/increasing predictability), including attention to productivity, coordination, cost and revenue.

"Predominantly institutional" was operationalized as the relative prominence of features or mechanisms that are associated with an institutional model of performance, i.e. regulative, cultural, and/or mimetic mechanisms. This construct relates to the ideas of new institutionalism, wherein the "environment as institution" constitutes the source of homogenizing mechanisms on organizations in the same field (DiMaggio & Powell, 1991; Zucker, 1987).

Institutional mechanisms described as regulative:

1. pressure *from external sources, e.g., professions, established business relationships, and government regulatory agencies*

Institutional mechanisms described as cultural:

2. diffusion of *social facts through the historical processes of a Delta business area, e.g., trust arrangements with resource suppliers*
3. influence within a Delta business area *from existing practices and routines relating to IT systems*

Institutional mechanisms described as mimetic:

4. imitation of solutions *via diffusion from external sources, e.g., vendors, consultants, or other organizations.*[69]

The model variables, and their descriptions, are presented in Table 3.

Table 3: Model variables

DEPENDENT VARIABLE
Y2K solution: Changes to *software systems* in Delta's functional business areas from 1997-2003.
INDEPENDENT VARIABLE
Environmental context
Task environment
Institutional (cultural and regulative) environment
OTHER VARIABLE
Response assessment
Institutional responses relate to: Regulations Existing relationships Belief systems Existing practices and routines Imitating the solutions of others *Rational responses relate to*: Organization (division of labor, coordination mechanisms) Goal orientation Planning (certainty of means) Decision-making based on efficiency criteria

[69] Mimetic mechanisms are especially evident under conditions of uncertainty, such as existed during the *Y2K* crisis.

Models of organization

According to an institutional model, organizations exhibit evidence of rational behavior; but, different from a model designed for efficient performance, organizations make decisions that can be attributed to both overt and subtle social pressures in organizational environments. Expectations of legitimate behavior prevent rational choice based on purely economic cost and benefit (preference) evaluation. Over time, a focus on legitimacy leads organizations as members of a field to demonstrate isomorphism. Processes that lead to isomorphism, especially evident in a crisis mode, include imitation of the actions of other organizations in the field, and pressures that emanate from other sectoral aspects, e.g., the State and professions. Institutional behavior may be rational or institutional upon analysis, depending on an assessment of the value of efficiency vs. legitimacy to organization survival. The institutional model favors legitimacy over efficiency. In each of the target sub-cases in this investigation, solutions were interpreted according to both an institutional system model and a rational system model.

Summary

This dissertation was designed to fill a gap in understanding by investigating the ways in which institutionalized environments influence actions to secure information systems in complex organizations. The chapter presented a statement of the research problem and justification for the setting at Delta, the study of *Y2K*, and a focus on Delta's Year 2000 Program.

The investigation was described as a case study, which included a multiple embedded-case design—its purpose being to compare the actions and contextual conditions of four Delta sub-unit business areas, and to evaluate the actions as rational or

institutional responses. Actions of the parallel business areas of Delta were conceptualized as *Y2K solutions*—the results of decisions that were made with respect to *software systems* over the period 1997-2003.

The evidence of different *Y2K solutions* among parallel business areas allowed investigation of the influence of *contextual conditions*. A value for the *response assessment* as either "rational" or "institutional" was designed to contribute to understanding the business area's concern for efficiency vs. legitimacy with respect to organization survival.

The research hypothesis was stated: *the Y2K solution in a Delta business area can be explained as an institutional response to contextual conditions, which is related to sector-based institutional mechanisms.*

A competing hypothesis was stated: *the Y2K solution in a Delta business area can be explained as a rational response to contextual conditions.*

CHAPTER 4

DATA COMPLEXITIES AND ANALYSIS CHALLENGES

The investigation of each of the cases entailed three stages. First, relevant information was collected from both primary and secondary sources to serve as data. In the second stage, the data were processed to facilitate its analysis. The evidence was organized by business area according to the three constructs: *Y2K solution, environmental context, and response assessment,* the variables that represented the "common rules for distinguishing phenomena from context" (Yin, 1982). This data organization provided the framework for comparison. Qualitative analysis software was used to assist in the process, especially in locating evidence of influential environmental factors. Finally, a comparative method identified the similarities and differences among the sub-cases with respect to the framework. The following sections provide details for each of these stages.

Data: sources and analysis

Primary sources of data included both the unpublished records from the Year 2000 Program obtained directly from Delta and information assembled through interviewing individuals associated with the organization. The unpublished records had been produced as written communication during the process of implementing Delta's Year 2000 Program. These records, which numbered over 7000 documents, were stored as digital files on CDs—as letters, emails, project reports, compliance reports, internal publications, presentations, interorganizational communications, government documents,

etc.[70] A list of the documents from this archive that were cited in this dissertation is provided as Appendix J. These records had been stored previously on Delta's in-house computers, and copied onto CDs for backup purposes. The discovery that the number of files was large, that their organization schemes were inconsistent, and that the files themselves possessed different characteristics, led to a number of different attempts to standardize them and thus manipulate them more easily for analysis.

The files were organized in two different ways on the CDs: (1) as various document types via Microsoft (MS) Windows OS directory/folder system, and (2) as records in Oracle database format. The file characteristics were different both in format types, e.g., text, PowerPoint, Word, PDF, etc, and in design of the document information. Documents lacked specific and uniform business area identifications. Therefore, data mining using easy search methods was difficult. The documents were first "reverse engineered" in order to put them into forms and categories that enabled more efficient searching. This involved creating algorithms in programming code to locate date fields, and keywords and then categorize the documents accordingly. However, many of the documents were document image files, esp. pdfs, and therefore, did not lend themselves easily to this kind of manipulation.

The MS folder structures gave the initial appearance of being well-organized and of containing excellent information. However, upon inspection, the knowledge management system (kms) that Delta used to organize the project documents had not been populated uniformly by business area. Neither had the structure been used in its entirety as it was designed. Upon reflection, this might have been expected because of the

[70] Originals of many of these records existed as paper documents that were stored in a commercial off-site storage facility. These paper originals were to be retained until some time in 2007.

origin of the database system. The kms was a commercial package, not specifically designed by or for Delta; thus it provided the opportunity for fine-grained project documentation, but in a very "one-size-fits-all" way. In the end, many of the folder structures that had appeared useful for this research were empty of content.

The language used in document content created a challenge as well. The Delta-specific jargon and acronyms in these documents rendered them extremely difficult to comprehend as an outsider. As the IFALPA "Jargon Buster" states,

> Aviation jargon is sometimes a confusing and frustrating language. … just one acronym alone (IFE) has several meanings depending on the area of aviation it relates to, for example, IFE can mean 'In-Flight Emergency', 'In-Flight Entertainment' or 'International Flight Engineers' (International Federation of Air Line Pilots' Associations (IFALPA), 2005).

Two methods helped to resolve this issue. First, it was necessary to create what became an extensive glossary in order to read the documents with understanding. A Delta employee generously agreed to a visit by phone periodically to provide definitions and interpretations of acronyms. However, this activity was even difficult for the employee from time to time, as the Year 2000 Program was becoming dim in his memory. Second, making lists of keywords and names of people, along with their associated roles and titles, also helped to locate and understand relevant information in the archives. The discovery and utilization of qualitative analysis software was an invaluable aid to reading and keeping track of the documents, and to analyzing them with respect to environmental factors.

As noted above, informants were also a key source of primary evidence. Over two dozen individuals participated in this study and served as informants. Project discussion and interviews took place beginning in January 2004 through the close of the investigation in 2007. Informants were individuals who had been associated with Delta,

either as participants in the Year 2000 Program or as persons possessing relevant information.

The first contact with Delta was in the fall of 2003, when the dissertation design was being considered. This contact resulted in a meeting in January 2004 at the office of Leo Mullin, Chairman of the Board of Directors at Delta. Information from the conversation with Mullin led to an understanding that Delta was a viable target organization for the investigation. Subsequent visits to Delta included meetings with *Delta Technology* CEO Curtis Robb, a "field trip" to the Technology Control Center and to other facilities that served as support for the massive complex devoted to computer processing for *Delta Technology*. Robb also arranged for visits with Walter Taylor, former director of the Year 2000 Program and with Spark Nowak, Delta's Chief Information Security and Privacy Officer. Many other interviews followed.

Over the course of this investigation, the organization became a very difficult research site because of its bottom line—Delta reported a $2.6 billion net loss on $12 billion in revenue for the first nine months of 2005, and had declared Chapter 11 bankruptcy that September.[71] Many Delta employees had resigned and moved on or retired. Of those who had new jobs in other places, some were extremely difficult to track down. In contrast, although a very difficult time at Delta, weathering the problems with cost cutting in the attempt to emerge from bankruptcy, many of the people who remained at Delta were motivated to support this dissertation. Layoffs and employee attrition had

[71] Between 1997 and 2003, Delta's net income of $302 million had turned to a net loss of $773 million, and the specter of being included among the reductions in the workforce was a very real presence after that.

led to a workforce that had to shoulder more than its normal share of duties, therefore, had less discretionary time to aid this dissertation.

Participation in the study typically consisted of one or two short interviews.[72] A signed consent form was exchanged prior to formal interview, which was a requirement of the Georgia Institute of Technology and its Institutional Review Board when performing research involving human subjects. The interview consent form, which guaranteed confidentiality of information to the informant, is provided as Appendix B. Individuals interviewed included executives from both Delta and *Delta Technology*, members of the Year 2000 Program team, and consultants—persons external to the organization who had information regarding the Delta organization, but were not strictly involved with the Year 2000 Program. These three classes of individuals included key employees from each of the business areas, and others who participated either directly or indirectly in the Program. Employee participants included individuals who provided Year 2000 Program coordination and leadership, employees who dealt with the technical issues first-hand, and administrators who had to juggle the normal business processes with the need to give priority to the Year 2000 mandate. In the process of uncovering information about *Y2K*, efforts were made to include employees who had worked at Delta for a long time, and those who represented other special interests, e.g., pilots. Informants are listed in Table 4, which includes brief details about the relationship of informants to the project and the dates of interviews. Note that most of the employees on the Year 2000 Program team held dual roles. It also should be noted that while not reflecting the makeup of the

[72] Exceptions were the interviews with two individuals: a *Delta Technology* employee who agreed to multiple brief chats via cellphone as he commuted home in the evening, and a former employee who provided multiple opportunities for information gathering—in person, by phone and by writing.

Year 2000 Program team, with only a couple of exceptions, all of the employees who were formally interviewed for this dissertation were male.

Table 4: Information about interviews and informants

INFORMANTS	TITLE AT INTERVIEW	DATES OF INTERVIEW / CONTACT
EXECUTIVES		
Leo Mullin	Chairman Delta Air Lines, Former CEO, Delta (1997-2004). Mullin provided overview information and set up contacts for obtaining Year 2000 documentation and further information.	Jan 27, 2004 Aug 15, 2004
Gerald Grinstein	CEO, Delta (2004-2007) Non-Executive Chairman of the Board, Delta (1997-1999). Grinstein enabled contact with Shirley Bridges, who in turn provided contact with other Delta employees.	Late 2005
Curtis Robb*	Sr. VP & CIO, Delta; and CEO, *Delta Technology* (2002-2005). Former CTO, *Delta Technology*. Robb introduced *Delta Technology*, its facilities and chief participants in the Year 2000 Program.	Apr 07, 13, 21, 2004
Walter Taylor*	Managing Director of Process and Technology, and Pilot, Delta; Former Director - Year 2000 Program, and VP-Airline Operations Portfolio, *Delta Technology* (1997-2004) Taylor performed the leadership and administrative duties for the Year 2000 Program.	Apr 07, 13, 21, 2004
Spark Nowak*	Chief Information Security & Privacy Officer, *Delta Technology* (2000-2006) Nowak provided overview of information security activities.	Apr 07, 2004
Harry Richardson*	VP, Systems Operations, *Delta Technology* (2000-2007) Met Richardson briefly on tour of Technical Operations Center.	Apr 13, 2004
Charlie Feld	Exec VP, EDS; Former acting CIO, Delta, and CEO, *Delta Technology* (1997-2001). Feld spoke about overall strategy and leadership for the Year 2000 Program. He provided a video of the company-wide meeting that kicked off the Year 2000 Program at Delta.	Mar 31, 2006
Shirley Bridges	Sr. VP & CIO, Delta, and CEO, *Delta Technology* (2005-2007), Former Sr. VP - Operations, VP - Air Operations Portfolio, *Delta Technology* (1990-2005). Bridges provided contact with *Delta Technology* employees, but declined interview herself, stating she possessed no relevant information.	Feb 13, 2007
YEAR 2000 PROGRAM TEAM		
Tim Mitchell	Manager, BCP, *Delta Technology,* Former Production and Field Services, Technology Portfolio Lead, Manager – Year 2000 Program Desktop Strategy Project, led rollover crisis management team. Mitchell had a broad view of the Year 2000 Project because of his involvement with enterprise-wide aspects. He was responsible for release of Year 2000 Program records from storage in 2007.	Dec 08, 2005 Jan-Jun, 2006
Barry Webb	*Delta Technology*. Former Technology Portfolio, *Y2K* Workgroup Engineering team. Webb was one of the first Delta employees interviewed; and he was directed by HR not to participate in this dissertation.	Jan 20, 2006

Table 4: continued

INFORMANTS	TITLE AT INTERVIEW	DATES OF INTERVIEW / CONTACT
Charles Gravitt*	Municipal court judge, Jonesboro, GA. Former Year 2000 PMO Managing Director, Hartsfield airport *Y2K* Director, member - IT Board, Delta. Gravitt provided important early history of Delta.	Oct 11, 2006
John Jacobi	EDS. Former VP – Customer Systems, Customer Portfolio lead, *Delta Technology*. Feld arranged contact with Jacobi.	Mar 15, 2007
Neal Morgan*	Retired. Former Customer Portfolio Lead (1997-1998), *Y2K* Remediation Director, *Delta Technology*, (1998-1999), member - Hartsfield airport *Y2K* team (1999-2000). Morgan led important Y2K initiatives for Delta.	Oct 28, 2006 Feb 03, 2007
John Mock	Former *Y2K* Technology External Agent Process team, *Delta Technology*. Neal Morgan arranged contact with Mock.	Feb 03, 2007
Eugene Shtern*	Consultant, Miratech (2006-2007) Former PMO Operations Portfolio rep (1997); liaison - *Y2K* code remediation project in Kiev, Ukraine, *Delta Technology* (1998-1999) Shtern was instrumental in saving Delta $12 million because of liaison with Ukraine consulting group. Neal Morgan arranged contact with Shtern.	Feb 03, 2007 Mar 25, 2007
Oscar Gallindo	IT security for ISN, consultant to Hartsfield *Y2K* project	Feb 03, 2007
Otis	Former Manager, City of Atlanta Aviation Department	Feb 03, 2007
Russ Morgan	EDS, Former Customer Portfolio, *Delta Technology* (1998-2006) Jacobi arranged contact with Morgan.	Mar 15, 2007
CONSULTANTS		
Jack McMillan	CEO, TechBridge, Former project leader on the Finance Reengineering project performed at Delta from 1990-1996. Following interview, McMillan introduced former Delta employees.	Sep 29, 2006
John Day	Retired. Former Partner in Charge of the Delta audit team, first with Arthur Andersen & Co, and then Deloitte Touche.	Oct 09, 2006
OTHERS		
Peter Wan	Sr. Information Security Engineer, Georgia Institute of Technology Wan provided broad context for history of IT, exp. related to information security.	Feb 05, 2007
Luke Ott*	Pilot, Asst deputy information security officer, Delta	Oct 30, 2003
Kelly Wills	Retired. Former Network Systems - Human Factors Team Mgr, *Delta Technology*. Wills made a presentation to the CHI-Atlanta organization where she described the development of Delta IT transformation with respect to HCI. Even though Wills had leadership responsibility within the Future Vision technology transformation, she declined interview stating she possessed no relevant information.	Jan 29, 2004
Jay Libove	Sr. Information Security Engineer, Information Security & Privacy Office, Delta	Oct 21, 2005
Tim King	Information architect, MacQuarium, Former Network Systems - Human Factors Team, *Delta Technology* King worked on the Customer Care system.	Feb 22, 2006
Judy Bean	Manager, Delta Air Transport Heritage Museum, Delta. Provided Delta in-house publications.	Jan 11, 2007

Table 4: continued

INFORMANTS	TITLE AT INTERVIEW	DATES OF INTERVIEW / CONTACT
Tiffany Meng	Curator, Delta Air Transport Heritage Museum, Delta. Introduction and brief interview while touring the museum. Her father being a 30 year Delta veteran, she grew up in the Delta "family."	Jan 11, 2007
Marie Force	Archives Manager, Delta Air Transport Heritage Museum, Delta. Brief interview while touring the museum.	Jan 11, 2007
Mary Raines	Retired. Lawyer in the Legal Department, Corporate Secretary, Delta. Raines declined interview, stating lack of involvement with *Y2K*, and total ignorance of IT.	Jan 2007
Juan Gomez-Sanchez	In charge of information security for the Delta website, *Delta Technology*. Gomez-Sanchez agreed to a date and time for interview by phone, and then did not answer his phone at the predetermined time, nor did he return subsequent calls.	

Interviews probed themes related to the investigation in a semi-structured way.[73] Themes associated with the institutional system model pertained to regulatory, cultural, and mimetic mechanisms. Themes that related to the rational-contingency model pertained to rational mechanisms. Attention was paid in the interviews to gathering information regarding the problems each of the Delta business areas encountered related to the Year 2000 Program (esp. any issues that could be characterized as externally induced), and the approach each business area utilized to address these challenges.

Secondary sources of data were previously published materials in the form of articles both from scholarly and trade publications, and books about Delta. These materials were publicly available in libraries, bookstores, websites, and electronic databases. Also included in this category of evidence were the Delta annual reports.

The process of analysis proceeded somewhat iteratively with data collection. Documents from the Year 2000 archive were investigated using content analysis, which

[73] An interview protocol guided the interrogation of informants. The protocol is attached as Appendix A.

began early-on by applying concepts and factors that were expected to emerge in the data, factors with strong association to the concepts of institutional and rational-contingency theory.

Then, analysis proceeded via an inductive process. Through a systematic process of reading, interpreting, and coding the documents using qualitative analysis software, a number of additional concepts were included. Table 5 summarizes the analysis process. A list of factors is shown in Appendix I.

Table 5: Data analysis process

	TARGETS FOR ANALYSIS	
	• Business area characteristics	
	• Organization of process, materials	
DATA	• Participant roles, relationships	**PRODUCTS**
Archival document contents	• Changing roles, responsibilities	Results of decisions, action items
- reports by business area	• Discussion topics, features	Goals
- Year 2000 team communications	• Sequences of events	Participants
- presentations to Delta executive management	• Mission statements	Participant perspectives
- communications within the air transportation industry	• Statements of objectives	Organizing themes, concepts
- public communications	• Repeated activities	Evaluative rules, criteria
Interview notes	• Cultural features	Organization facilitators
Journal articles	• Evidence relating to beliefs	Organization constraints
Trade publications	• Evidence of conflicts	Power and status systems
Video of company meeting	• Patterns in communications	Regulative organizations
Books	• Use of language, word choice	Financial consequences
	• Evidence of rule following	
	• Decision processes	

In the attempt to discover causal factors for actions, the investigation compared the context and content of *Y2K* response actions among the four Delta business areas as

embedded sub-cases. The structure of the Year 2000 Program paralleled the organizational structure in Delta's business areas, which in turn facilitated the sub-case comparison. This Program structure served to define the project elements in each sub-case according to business area Portfolio assignments. The project elements included resources, roles and responsibilities, as well as project methods and metrics. The challenge was to locate information in the archives and, to discover and locate associated employees. Each sub-case entailed fieldwork and follow-on analysis of data. The subsequent discovery of environmental factors was the result of a process that was both deductive and inductive.

Comparative case study method

The comparison of the four sub-cases was designed to address whether or not the same relative causes could explain the differences in solutions that four business areas adopted in dealing with the same problem. The method of analytic comparison (Mill's method of difference) formed the basis for cross-case comparison.[74] The analytic comparison process systematically compared sub-cases to determine those that were similar with regard to solutions and causal factors with others that differed on solutions and causal factors. The method provided the ability to find sub-cases that had the same causal factors and solutions but lacked a few key features, then through a process of elimination, to locate factors common to them all.

Using this method, variables representing the two competing models were examined, the institutional system model and the rational-contingency system model. According to an institutional system model, the influence of environmental context leads

[74] Neuman (2000) describes Mill's logic. For further discussion, see also Ragin (1987).

to sub-optimal organization decision-making (institutional responses) with respect to efficiency and predictability. Conversely, according to a rational-contingency system model, optimally structuring the organization and its processes (rational responses) maximizes the efficiency of operations and its coordinating mechanisms.

Summary

This chapter described the data and its sources, and the method of analysis. Primary data sources were the archived records of Delta's Year 2000 Program, and interviews with various people associated with Delta. Secondary sources were previously published materials. The chapter described the approaches used to organize the data and to analyze the data for environmental influences, and the challenges encountered in attempting to understand and organize Delta's written records. Qualitative analysis software was used to facilitate analysis, which involved the coding of concepts that were identified in the documents and the interview reports. Following organization of the evidence, a comparative method was applied in order to compare the solutions and factors across sub-cases.

CHAPTER 5

THE CASE OF DELTA AIR LINES: ITS CRITICAL INFRASTRUCTURE

> Three weeks after Leo Mullin joined Delta as chief executive in 1997 he learned that the airline had the worst technology in the business. No one was sure that Delta would survive the year-2000 calendar change (Corcoran, 2000).
>
> [Delta] would never have achieved what we did without *Y2K*. … and, 9/11 still has great impact. Delta was very involved at the time and it still strongly affects us. We instantly changed from a $16B to $13B company. If it happens again, we can't survive (L. Mullin, 1998, Jan 27, interview by author, Atlanta, GA).

This chapter presents background information on the Delta corporate organization in broad historical, cultural, and environmental overview, and more specifically with respect to the Year 1997, the year when the Delta Year 2000 Program was announced formally.[75] Attention is given to issues related to Delta's growing dependence on information technology and to issues related to the management of its IT systems. This overview establishes the context within which the Year 2000 Program took place.

Historical overview

1924-1997

This section provides a brief chronological accounting of the history of Delta and its industry environment from 1924 through 1997, these years representing the beginning of the company and the beginning of the study period, respectively. A more complete chronology of Delta's history is available in the Timeline (p. xxxvii), which presents milestones in Delta's operations during this period and after. It is interesting to reflect on

[75] Information and statistics in this section are taken from the following: Delta annual reports, from Jones, G. (2003), and from Bitran, Gurumurthio, & Sam (2006).

how far Delta and air transportation technologies have advanced, considering that the year 2003 marked one hundred years since the Wright brothers' flight. The early activities at Delta came around 20 years later.[76]

Delta began as a crop dusting firm in Macon, Georgia in 1924. Two young men with different skills, but innovative ideas, started the business with very limited capital—sounds like the experience of Jobs and Wozniak. However, in contrast to the beginnings of Apple Computer, the innovation of the Delta founders, Dr. B. R. Coad and C.E. Woolman, came through the new technology of aviation, and required no expertise on the part of the customer.[77] However, expertise on the part of the *managers* of this business must have been strong, as this air transportation company has weathered many storms over the years, yet stayed the course.

The founders expanded the crop dusting business into transporting passengers in 1929, five months before the stock market crash that set off the Depression.

> The five-passenger, 90-mile-per-hour Travel Air launched Delta's passenger service on June 17, 1929. ("A History of Service," 2003).

Then nine years later, legislation was passed that would prove to be a pivotal event for Delta's future. Beginning in 1938, Delta (along with the rest of the airline industry) was required to operate under the control of the federal government regarding its fares and routes.[78] For the subsequent forty-year period under the new regulation, the air transportation industry settled in and developed into a valued element of U.S. infrastructure. This was a period of both stability and growth for Delta, which included

---

[76] As another reference point, the activities that are the subject of this research took place around 20 years after the introduction of the personal computer.

[77] The crop dusting business would remain intact until Woolman's death in 1966.

[78] Prior to the passage of the Civil Aeronautics Act of 1938, airlines had been free to operate with no regulation other than regulations that promoted safety.

developing its first computer systems in-house. However, federal regulation of the airlines reduced the need to focus on efficiency in operation and ultimately permitted the industry's payrolls to expand; these realities added to the mayhem when the regulation was reversed.

In 1978, President Carter reversed the government control by signing the Airline Deregulation Act, which eliminated most domestic economic regulation of passenger and freight services and returned airlines to free competition on ticket prices and routes. The act resulted in such a shakeup in the industry that bankruptcies became common, adding to the chaos and uncertainty in the marketplace.

> The fuel crisis of 1979, the air traffic controllers' strike of 1981, the severe recession in the early 1980s and the intense price competition combined to produce the worst losses in the history of domestic aviation. During the first decade of deregulation, more than 150 carriers collapsed into bankruptcy. ... In part due to the Persian Gulf War in late 1990 and the end of leveraged buyouts in 1989, the industry again experienced a serious downturn (Bitran, Gurumurthio, & Sam, 2006, p. 2).

Even though Delta had suffered economic losses during this time, the organization survived by making organizational changes, which reflected its capacity to adapt in the new competitive environment. This adaptation became a pattern that has been observed in its more recent management strategies.

> After thoroughly analyzing the harsh financial pressures and the competitive reality of low-cost carriers' continued expansion, Delta embarked upon an ambitious and accelerated journey to reinvent and redirect itself. Our goal is to meet the competition head-on by becoming a more efficient and simplified airline uniquely designed to improve the customer travel experience while simultaneously cutting costs (Grinstein, quoted in Delta Air Lines, 2004).

Over the next 20 years that preceded the Mission Possible: Year 2000 Program,[79] the Delta internal organization, as well as Delta's sectoral environment, experienced a

[79] "Mission Possible: Year 2000 Program" was the name that was given to Delta's Y2K project. In this study, the name of the project is simplified to "Year 2000 Program."

number of changes in response to the changes brought about by deregulation. During this time Delta gradually began to uncouple in-house functions—in keeping with popular ideas about focusing on core activities and outsourcing the rest, the rest including those associated with IT investments.[80] Delta IT investments had become significant fixed costs; therefore, were examined with respect to streamlining the business and increasing operating efficiency. Further, Delta's strategy turned to plans for employing functional assets for generating revenue, rather than limiting them to the support of Delta's own business activities. As part of this strategy, for a brief time Delta attempted to market its software assets as a source of revenue.

In-house management of IT systems

> Through the mid-'90s, much of Delta's operations ran on spreadsheets and checklists. Pneumatic tubes were used to shuttle information throughout airports. What systems were in use were scattered and disconnected (Overby, 2003).

By the mid-90s, the Delta organization was heavily dependent on technology, its greatest dependence being its aircraft. In order to operate the aircraft, Delta's pilots and mechanics had to stay current with the increasingly complex aircraft technologies, which involved training and certification. However, managing aircraft technologies was just one of the highly complex technologies that the organization had to stay on top of continuously in order to stay in business. Among its daily challenges was managing its IT systems.

Delta's dependence on IT goes back to the 1964, when IBM developed and installed the Deltamatic flight reservation system for Delta (Smithsonian National

[80] Catering operations is an example. Many airlines sold these operations years ago as part of a plan to focus on core activities (Moorman, 2004).

Museum of American History). However, beyond this earliest effort to engage IT to support the business, it was rare for Delta's management to call on the expertise of outside vendors for help with systems' maintenance. The CIS department generally resisted using consultants. As one retired employee said, "We wouldn't touch them with a ten foot pole!"

Over the years that followed, hundreds of other business software systems and technologies were developed and installed in piecemeal fashion, of which—like most organizations of Delta's age and size—a large percentage had taken place in-house. In-house development was common, simply because few or no commercial applications were available until sometime in the early to mid 1990s. Over these earlier years, Delta business areas had developed their computer systems internally rather than to contract with outsiders. Delta and many other organizations felt their systems were so specialized and critical to their operations that they chose to develop them in-house. However, more realistically, the special issues in the air transportation industry, coupled with the limited number of airline companies, necessitated custom applications in many areas. Further, the philosophy of custom in-house development would extend into areas where there were better commercial off the shelf (COTS) solutions on the market, such as business support and customer service software. Moreover, by 1997 the systems were no longer working together effectively to coordinate and facilitate the increasingly complex functional activities. This situation compounded the complexity of the organization and reduced its operating efficiency.

Delta's core business areas— *Airport Customer Service, Operations*, *Business Support*, and *Revenue*—all had unique needs for processing information. In addition,

Delta's systems were isolated in functional areas of the organization, many incapable of interaction. Therefore, the systems had become limited in their ability to provide accurate, timely information about flights and to coordinate information between users who needed it. Historically, business area priorities for whatever reasons had put the CIS department way down the list resulting in less than state-of-the-art systems. For example, Delta's own reservations systems were long in coming, and, some would say, inferior upon arrival (Petzinger, 1996). These different technology circumstances would influence business areas in how their problem was defined for *Y2K solution*. In addition, Delta's financial difficulties since deregulation had created a focus on reducing expenditures, which had created distrust among employees in different Delta business areas.

During the 1990s, the vulnerabilities in Delta's information systems—made more pressing by the *Y2K* bug—eluded resolution by the Computer and Information Services (CIS) department. Typical of many complex, institutionalized organizations, computer-based systems at Delta developed according to an incremental process and over time had not kept pace with changing technologies. In the midst of this high technology environment, Delta had trouble dealing with the vulnerabilities in its information systems. The expertise of IT staff matched the state of the systems. This was to be expected. The employees who managed the systems possessed the knowledge that was required to perform their duties. However, the world of software production had advanced since the code in many of the systems was written. Delta's training personnel had also become deficient in staying abreast of the latest technologies; therefore, the situation could not mend itself internally.

Having been in the air transportation business for over 70 years, change at Delta had become difficult (especially to its information systems) and, competition was intense. As a result and contrary to the notion of controlling cost, parts of the organization operated according to decades-old patterns, and were incapable of improving profits with their current production systems. Within this organizational environment, attempts to improve the IT function enterprise-wide had come in fits and starts and amid uncertainties; so that, mired in its own history, Delta had been unable to pull itself forward.

Outsourcing systems management

> While all GDS[81] computing platforms are essentially the same—big IBM mainframes running on the 40-year-old Transaction Processing Facility (TPF) operating system and doing everything from holding airline ticket inventories to handling transactions—Worldspan has aggressively moved some application software to faster, less-expensive servers. In January 2002, it shifted its fare and pricing applications to servers running Microsoft Windows NT (McCormick, 2003).

Beginning in 1990, Delta began to outsource portions of its IT services. Executive management had spent time with organization guru Mike Hammer, who encouraged the notion that an organization should focus on its core business, and should let an outside entity that specialized in the non-core functions do the other part. In addition, Delta's executive management believed that outsourcing was a way to fix some of the issues they had with their IT shop.

First, Delta entered into partnership with Northwest Airlines, TWA, and ABACUS Distribution Systems to operate and market Delta's computer reservation

[81] Computer reservations services (CRS) are also called GDS (global distribution services), which reflects the expansion of these kinds of services internationally.

system (CRS) under the name of Worldspan.[82] Following the outsourcing agreement, Worldspan provided CRS services to Delta; and Delta in turn provided communications, information processing, and administrative services to Worldspan.

The second project that outsourced IT activities came during the December quarter of 1994. Delta announced a joint venture and outsourcing contract that formed *TransQuest*, a new company operating in partnership with AT&T Global Information Solutions that would provide for Delta's IT service needs.

> Part of the charter is to move Delta away from legacy systems to a client/server architecture, according to company officials, who estimate that the venture will yield productivity gains that will save Delta $400 million over the 10-year period (Stackpole, 1994).

The IT organization began with the hiring of 1,800 personnel from within Delta's computer services group and a $300 million annual budget.

In forming *TransQuest*, Delta envisioned that the new company would not only provide IT services for Delta, but would also sell its services to others in the travel and transportation industries. At the outset, the company's focus was on three areas:

1. improving the quality and productivity of Delta's system development process,
2. installing a new IT infrastructure and,
3. cutting costs.

In its first year of operation, *TransQuest* had made major contributions toward meeting these goals. Toward addressing the first goal, *TransQuest* had improved its ability to satisfy end-user needs and shorten application development time by using object-oriented

---

[82] Travel agents are the primary users of CRS services, which enable electronic booking for airline, hotel, car rental and other travel reservations and issuing airline tickets. CRS services are provided by several companies in the U. S. and worldwide. In the U.S., other CRS competitors are SABRE (owned by American Airlines, Inc.), the Galileo International Partnership (owned by United Air Lines, Inc., USAir, Inc. and certain foreign carriers) and System One AMADEUS (owned by Continental Airlines, Inc., AMADEUS and EDS).

programming technology. Toward addressing the second goal, *TransQuest* had nearly completed deployment of an enterprise-wide, three-tier client-server system to integrate and standardize Delta's systems, and to provide common data that supported the users in multiple business areas.

> The Atlanta-based company has turned to IBM's MQSeries to tie together applications on a rainbow of different platforms and drastically cut application development costs, said Mark Whitney, senior fellow for middleware at TransQuest, Delta's information systems arm. “Now we can gather all our disparate information and drop it into a queue and bring it into one database,” Whitney said. “You can begin to join information you never could join before.” TransQuest will also use MQSeries for several other projects that let Delta's widespread client/server applications converse with the Transaction Processing Facility (TPF), the central airline process system running off an IBM System/390 mainframe. These include electronic ticketing and reservations and information kiosks located in airport terminals, all which require secure, unbroken communications (Ouellette, 1996).

By then *TransQuest* had made the decision to install Windows NT operating systems in desktops units, and it was important to assure that the middleware functioned properly in connecting with end users. Therefore, the organization was also considering testing middleware from Microsoft that could help its Windows NT desktops exchange data with a slew of legacy systems. Although *TransQuest* had purchased MQSeries for Windows NT, its client platform of choice, the firm also was interested in Falcon, Microsoft's middleware for Windows NT, which would not available until the following year. With continued cooperation between IBM and Microsoft on the project, *TransQuest* hoped to run both Falcon and the MQSeries middleware. Computerworld’s Ouellette (1996) interviewed Mark Whitney, who was then a senior fellow for middleware at *TransQuest*, about this.

> We are delighted with the cooperation between IBM and Microsoft on MQ-Series. … That is a positive, because we have such a heterogeneous environment and don't want to make a choice between one or another vendor.

That same year, *TransQuest* also had established the Operations Control Center (OCC) in the Operations business area, which improved flight monitoring and air traffic control, and offered the opportunity to trim the cost from flight delays (Caldwell, 1997). However, the cost-cutting goal was yet to be accomplished. Table 6 shows Delta's percentage ownership in the partnership companies at June 30, 1996, which reflects earnings (losses) for fiscal 1996, 1995, and 1994.

Table 6: Delta percentage ownership in associated companies

		EQUITY EARNINGS (LOSSES), $MILLIONS		
	Ownership, %	**1996**	**1995**	**1994**
Worldspan	38	$(5)	$(4)	$1.
TransQuest	50	(8)	(3)	-

Source: Delta Air Lines. (1997).

On July 1, 1996, the partnership was dissolved; and, *TransQuest* became a wholly owned subsidiary of Delta.

Delta Air Lines in 1997

Long before 1997, it was clear that Delta's information systems had begun to contradict the outward competence evidenced by the airline's many years of successful operation. By 1997, Delta had demonstrated remarkable endurance as an enterprise despite the deregulation shakeup. As noted in the Timeline, Delta had weathered its economic trials by strategic action that represented both technical and institutional endeavors, and in the process had recorded a number of air transportation "firsts."

Continuing this forward momentum, a number of prominent events occurred in 1997. Having come through some difficult years through the 1980s and early 1990s, Delta was in excellent financial shape in 1997. The 1997 Annual Report shows that fiscal

1997 was the best financial year in Delta's history. In that year, Delta had reached a milestone in aviation history in transporting 100 million customers in a single year. No commercial airline had ever achieved this. In 1997, Delta made major change to its insignia for the first time in 35 years. There also was a change in its auditing relationship. After 52 years of successful partnership with Arthur Andersen & Company (AA&Co), Delta named Deloitte & Touche as independent auditors.[83]

The year 1997 witnessed the retirement of President and CEO Ronald Allen after serving for 14 years in that post, and for a total of 34 years with the Delta organization. Allen's replacement, Leo Mullin, represented a change in philosophy of the administration, as evidenced by three major differences from prior CEOs. As the first major difference, Mullin was the first person to lead the company that had not been promoted from within the organization. Second, even though Mullin had worked in the transportation industry, he came with no experience with an airline company at all.[84] Third, different from previous CEOs, he came with extensive experience in IT that went back to the beginning of his career.[85]

Mullin (2004) described the posture of the organization with respect to Y2K when he first arrived in the fall 1997:

---

[83] As auditors of Enron, the entire global firm of AA&Co was forced to cease operation because of the collusion of a few of its principals in Enron's fraudulent activities, a court ruling that would later be withdrawn but too late to save the firm.

[84] Mullin had served for five years as Sr. VP for Strategic Planning at Consolidated Rail Corporation (Conrail) in Philadelphia, a company offering freight rail service.

[85] Early in Mullin's career, he spent 9 yrs. with McKinsey & Co.

> The company was extremely serious about Y2K. In fact, I would call it a crisis mode. The situation was very threatening due to the condition of the existing information systems. The major questions for all concerned had to do with identifying the issues. By far the biggest problem was setting priorities on what absolutely had to be done by January 1, 2000. Pent up ideas and demands from various entities had to be sidelined in order to focus only on tasks that were essential for assuring compliance and continued operations. The company helped these entities to understand the rationale for priorities and why their needs had to wait.

Table 7 shows the state of the Delta organization as of 1997 and 2003, representing organizational statistics at two milestone events: the employment of Leo Mullin as CEO, and Mullin's retirement [after Delta had spent $1.6 billion on IT improvements (Robb, 2004, Apr 21)], respectively.[86] See Appendix C for an organization chart of management in late 1997.

Table 7: Delta organization statistics at the beginning and end of the study period

	1997 *(BEGINNING)*	**2003 (*END*)**
Employees	63,400+	70,600+
Aircraft	553 (14 types)	833 (15 types)
Operating revenue, $millions	$13.6 billion	$13,303
Operating expenses, $millions	$12.1 billion	$14,089
Passenger mile yield	12.79¢	12.49¢
Avg. fuel cost/gal	66.28¢	81.78¢
Independent auditors	Arthur Andersen & Co [87]	Deloitte & Touche LLP
Delta + partners daily flights	4,800+	7,100+
Destinations	149 domestic cities in 42 states, the District of Columbia, Puerto Rico and the U.S. Virgin Islands 41 cities in 25 countries	206 domestic cities in 47 states, the District of Columbia, Puerto Rico and the U.S. Virgin Islands 48 cities in 32 countries
Revenue passengers, millions	101.148	104.452

[86] Mullin accepted the role of Delta's President and CEO, and a membership on the Board of Directors, immediately following the official launch of the Year 2000 Program in July 1997.

[87] Arthur Andersen & Company had served as independent auditor of Delta for 52 of its 70+ years.

Table 7 continued

	1997 *(BEGINNING)*	2003 (*END)*
***Delta Connection* carriers**	Atlantic Southeast Airlines (ASA) Business Express Comair SkyWest.	Atlantic Coast Airlines (ACA) Atlantic Southeast Airlines Comair Chautauqua Eagle Freedom America Delta Shuttle SkyWest Song
Alliances	Atlantic Excellence alliance Swissair Austrian Airlines Sabena South American alliance Transbrazil	SkyTeam alliance AeroMexico Air France Alitalia CSA Czech Airlines KLM Royal Dutch Airlines Korean Air Marketing alliance Continental Airlines Northwest Airlines
Code-share partners	Air Jamaica Avianca China Airlines China Southern El Al Israel Airlines Royal Air Maroc South African Airways	Air Jamaica Avianca China Airlines China Southern El Al Israel Airlines Royal Air Maroc South African Airways

Source: Delta Air Lines (1997), Delta Air Lines (2003).

Cultural character

In addition to Delta's history, its culture was an important element of context for the Year 2000 Program. Three prominent institutional characteristics among Delta employees were identifiable in Delta's culture:

- view of themselves as "family," and
- experience in military organizations.

The next sections discuss these features in turn.

Family

For much of its history, Delta employees had considered themselves "family." As an example of family loyalty, in the economic downturn of 1981 and 1982, when Delta was in financial trouble, employees raised $30 million to purchase a plane, enabling Delta to make good on an order that had been placed at an earlier time when all was well. The plane, a Boeing 767-232, entered service in 1983 and was named the "Spirit of Delta."[88]

Even though in this example Delta employees may have represented a cultural extreme, the family culture was the norm among large corporations for much of the 20th century, where employees expected to work their entire careers with the support and protection of their firm. Organizations tended to hire for life, and employees shared a similar sense of loyalty. Companies celebrated the tenure of long-term employees; they took care of their people by providing health benefits, pay raises, and retirement funding. Following de-regulation, Delta tried to hold on to this paternalistic view quite a bit longer than most companies of that era.

Over the years, as in any family, there were sources of conflict, particularly during times of financial hardship. Under these circumstances especially, the pilots' union had played a particularly adversarial role. It might have been the Delta family spirit—and the underlying incentive systems at Delta—that united the employee community and preempted the need for unionization of most of the workers. However, Delta pilots had come to expect the high pay and benefits they had enjoyed over the years as the privileged "kids" in the family; pilots seemed to behave as "spoiled brats" in

[88] The Spirit of Delta was housed in the Air Transport Heritage Museum, located in Delta's original Hangar One at Hartsfield Atlanta International Airport.

Delta's continuing attempts to lower costs and compete with the newer airlines that became prosperous following deregulation.[89] Some have described the Delta family as having two components, the pilots and everyone else. Nevertheless, Delta employees were accustomed to this situation with the pilots, and often blamed not the pilots, but the Delta administration ("Mom and Pop") for the pilots' favorable economic status. The story goes that at one point, the pilots' union demanded that Delta provide pilots with limousine service to and from the airport, and that this benefit be written into their contracts. However, in this case, Delta administration prevailed, arguing for greater equality of privileges for all the groups that made up the Flight Operations division.

In addition to issues with pilot conflicts, over time Delta had added enormous complexity to its operations and processes—through mergers and acquisitions, increasing numbers of affiliations, and various additions to aircraft and computing technologies—to which many employees had become accustomed and saw as normal. In 1997, a large percentage of the workforce had been in the organization for 20 years or more. Therefore, many were potentially able to assess this cultural persistence at Delta.

Military

> The aviation industry has evolved out of a military base. Much of our management style, marketplace orientation and paraphernalia of culture still reflect an authoritarian, hierarchical and command-and-control worldview (Shackford & Shackford, 2003).

This mentality, like other aspects of the air transportation industry, has strong ties to the military, another cultural environment where strict control is emphasized. Because of their common use of airspace, among other reasons, Delta's wider environment

---

[89] Lower cost airlines operate with a different culture and employ a point-to-point route system instead of the hub-and-spoke system. "A major hub-and-spoke airline such as Delta has costs that can be 150% higher than those of a carrier that only flies from one city to the next" (Gage & McCormick, 2003).

included military organizations. Within its "family" environment, Delta had developed a tightly coupled cultural model over the years for very sensible reasons. Safety was strongly emphasized as a part of the air transportation mentality such that Delta had built into the culture strict controls incorporating attention to detail.

The abundance of military pilots trained for service in WWI helped to establish the beginning of the air transport industry after the war ended. In 1942, Delta contributed to the effort in WWII by modifying over 1000 aircraft, performing maintenance operations, and training pilots and mechanics. As noted in the Timeline, Delta carried passengers and military cargo during the first war in Iraq in 1990-91. More recently, Delta was a participant in the Civil Reserve Air Fleet (CRAF) Program during the period beginning October 1, 1997 and ending September 30, 1998, whereby the company agreed to make available up to 21 of its international range aircraft for use by the U. S. military related to national emergencies (Delta Air Lines, 1997, p. 10).

Many Delta employees, particularly in the *Operations* business area, received training in military organizations prior to joining Delta. "80% of Delta pilots are former military" (Shtern, 2007). Other employees in the Flight Operations division (e.g., communications technicians) and Technical Operations (e.g., mechanics) in many air transportation organizations often have military experience prior to joining a civilian activity. An example is the transition of Admiral James Loy directly from the military to Undersecretary of Transportation for Security, a post in the Department of Transportation (DOT).

> Loy, who retired as commandant of the Coast Guard the same day he was tapped for TSA. … TSA is focused for the moment on aviation security and airports because of the way the ATSA [Aviation and Transportation Security Act, which called for the creation of TSA] was written, but eventually we want the national transportation system writ large to be the benefactor of a higher security profile (Scalet, 2003).

Military environments are institutionalized, and their cultures are well known in terms of rule following and behavioral expectations. Military culture supports routine ways of performing and discourages innovation. An array of military organizations (e.g., U.S. Army, U.S. Air Force, British Navy, and Army of the PRC) likely exhibits similarity in structures and processes, similarity that derives from conformity to what is understood to be legitimate in the industrialized military field rather than evidence of effectiveness. Can it be said that the British lost the war of American independence because of its strict reliance on structures and processes that were institutionalized in British military culture? An institutional system model may explain actions of military organizations.

The enduring culture embedding those with military experience creates a sense of rule following and behavioral expectations in an organization that is likely different from the non-military experienced employee. Further, if the organization's dominant coalition were embedded in military culture, which is characterized by its highly rationalized model of planning, management, communication, and adaptation, the rules and behavioral expectations for the organization would be influenced by this. (Note: If the organization in total is influenced by military culture, then there should be no variation among business areas, except that related to technical function.)

Military organizations are mission driven. Each sub-unit has a clearly defined mission. There is a high degree of bureaucratization and delegation, from the highest level down to lowest sub-unit. Each person knows where he fits and what his job is. Military organizations employ a command and control management structure, with top down control and communication. Every sub-unit is expected to conform to the chain of command without independent strategizing. As a rule, military organizations are oriented

toward contingency planning—advancing thought to various alternative responses and plans. Even though tightly structured, there is the expectation of adaptation to immediate circumstances at each level of command structure. Therefore, constant communication is a requirement for execution of duties. Information and feedback continuously travels back and forth from top to bottom and bottom to top through the chain of command.

Labor organizations

Over the history of Delta, labor organizations were absent from the Delta ranks except among the pilots. In 2002 Delta could still be proud of the fact that besides the unionization of the flight superintendents (approx. 200 employees), the pilots' union was the only union represented in the company.

> Delta's operating advantages include having only one union, the pilots'. Flight attendants in 2002 rejected unionization by a vote of 71 percent to 29 percent, and ramp workers rejected it for a second time in 2000, 83 percent to 17 percent. Mullin, who is from Boston, credits Delta's "Southern heritage," meaning a sense of graciousness that has become, among employees, a kind of "covenant" (Will, 2003).

The flight attendants and other *Operations* groups had successfully voted down attempts to unionize.

All of these cultures—military, family, and labor organizations—have a high degree of loyalty. However, in military culture, different from that in a family or a labor union, mission trumps individual rights. Like military organizations, Delta historically had promoted from within. However, because of severe profit pressure in the later years of Allen's leadership, morale and customer service had been negatively impacted and changes were needed. Like in a traditional family culture, when problems were at an impasse, outsiders were hired to try to fix them. Mullin was an outsider and a non-military employee. However, the executive in charge of operations, Mac Armstrong, also

an outsider, was a retired U.S. Air Force (USAF) General.[90] Walter Taylor, the director of Delta's Year 2000 Program, was an outsider and a former USAF pilot.[91] *How many others in the executive ranks were new to Delta at the time of Y2K? … were military? Did outsider leadership significantly affect the Year 2000 Program?* Answers to these questions, while not a part of this investigation, are indirectly relevant to *Y2K* solutions. However, toward illuminating the factors of direct interest to this dissertation, the next section addresses the situation with respect to the influences in Delta's external environment.

Sectoral environment

> This is an especially good time for you vacationers who plan to fly, because the Reagan administration, as part of the same policy under which it recently sold Yellowstone National Park to Wayne Newton, has "deregulated" the airline industry. What this means for you, the consumer, is that the airlines are no longer required to follow any rules whatsoever. They can show snuff movies. They can charge for oxygen. They can hire pilots right out of Vending Machine Refill Person School. They can conserve fuel by ejecting husky passengers over water. They can ram competing planes in mid-air. These innovations have resulted in tremendous cost savings which have been passed along to you, the consumer, in the form of flights with amazingly low fares, such as $29. Of course, certain restrictions do apply, the main one being that all these flights take you to Newark, and you must pay thousands of dollars if you want to fly back out (Barry, quoted in Lu, A. C.-J., 2003, p. 1).

> Business units fully understand that the Year 2000 problem, if left unresolved, would result in business failures, loss of opportunity, extreme customer dissatisfaction and litigation. … The business units recognize this is not just a technology problem. External dependencies, where there is little to no influence, pose an even greater risk to Delta's operation (Delta archive, "Delta Year 2000 Program Briefing Book," 1999, p. 4).

The business of Delta Air Lines is conceptually simple: transporting passengers and freight from one place to another via aircraft. What makes it difficult is the vast numbers of aircraft—of many types, owned and operated by many others—who share

---

[90] Armstrong came to Delta as a 31-year military aviation veteran. He had retired from the Air Force as a three-star general in 1995.

[91] Taylor had actually come and gone and come back, but had accrued little service time with Delta.

common spaces, both in the air and on the ground. Among the aircraft operators are numbers of both military and civilian organizations, all of which are responsible for critical public infrastructure services. Because of the critical nature of air services—therefore the importance of safety and reliability—a number of government agencies and industry affiliations provide regulatory oversight for the aviation system.[92]

To manage the common spaces, a conspicuous mass of regulations and standards have been developed, along with government and industry agencies that monitor air transport-related entities with respect to compliance. However, many of the agencies that were created principally in the interest of safety have become dependencies upon which airlines rely in order to perform their services. Further, by 1997, many of these agencies had become dependent on computer-based processors and were likewise dealing with the risks of *Y2K*.

Government agencies

> The airlines now have the network infrastructure and planes, but airports and ATC [Air Traffic Control] systems [are] inadequate (Mullin, 2000, p. 7).
>
> [O]ur airports and ATC systems remain woefully inadequate, both in capacity and in many measures of operational performance. We are continuing to work closely with governmental representatives to find solutions that will fix the interrelated ATC problems of uncertain funding, inadequate equipment, an unresponsive organizational structure, and outmoded systems (Mullin, quoted in Delta Air Lines, 2000).

Government regulations principally center on safety, but also focus on routes. Safety regulations were designed to protect the safety of the aircraft, the crew, the passengers, the mechanics, the ground handlers and equipment, the jet fuel, and other

---

[92] The aviation system comprises airports, aircraft, air traffic control, airspace, and air travelers. Within these elements are pilots and passengers, control systems for approach and routes, control towers, and various categories of ownership of air transportation services: military, corporate, commercial, and general, along with various types of aircraft.

aircraft that share the same spaces, the spaces being the airspace, the buildings and runways of airports, the nation-states over which and in which the aircraft travel, …, the list goes on. Route regulations deal with two main issues: safety, and sharing in the commercial marketplace.

First, in the interest of safety, a plane needs a place to land in case of emergency. In the U.S., more than 10,000 airports serve a variety of flight-related activities, ranging from large complexes with several runways and many types of aircraft operations, to small air strips that can only accommodate light aircraft. Routes were established in order to limit the chances for traffic congestion, but also to enable access to an airport under emergency conditions. In earlier times, long distance routes for commercial aircraft were designed around the capability of the aircraft. Safety requirements dictated the route based on traveling only so far away from an emergency landing spot. Therefore, to deal with these issues government agencies evolved from the municipal-level on up to the federal level in order to regulate and monitor the air traffic.

Next, with regard to sharing in the marketplace, government oversight prevents airlines from flying at will to any destination they might desire. Delta's acquisition of the NY-London route from United in 2006 serves as an example. The agreement was subject to U.S. Department of Transportation (DOT) approval. The origin of this situation dates back to a 1977 treaty between the U.S. and the U.K. In this bilateral air transport agreement, the U.K. restricted use of the U.S. – U.K. routes in order to prevent U.S. domination in the global industry. Therefore, a formal process exists wherein the rights to fly between certain airports are conferred to a limited number of entities.

In order to accommodate air traffic lanes, as well as to accommodate passenger and cargo services, the schedules of air transport (time, place, date) must be accurate and reliable. From 1997 to 2003, the period during which the Delta *Y2K* solutions were planned and implemented, a number of air transportation regulations, professional certifications, and guidelines existed that may have influenced the way business areas organized and developed their IT systems. The following paragraphs present a selection of government regulators: FAA, DOJ, DOT, the U.S. Postal Service, and others.

The Federal Aviation Administration (FAA) is the chief regulator of public air space. The FAA regulates Delta's general flight operations affecting air safety, including the control of air space, flight personnel, and aircraft certification and maintenance, and other air safety concerns. FAA also regulates "slot allocations" at four major U.S. and certain foreign airports served by Delta. Each slot represents the authorization to land at or take off from the particular airport during a specified time.

In accomplishing its mission, especially regarding the control of air space, FAA employed computer-based systems that were questionable and worrisome during Delta's *Y2K* management program.

> Modernization of the U.S. air traffic control system has been a disaster story of epic proportions. The General Accounting Office estimates the cost of the push to modernize its information systems that the FAA started in 1981 will top $45 billion by 2005 (Carr & Cone, 2002).

Other regulatory bodies monitor and regulate certain competitive aspects of the airline industry. The U.S. Department of Justice has jurisdiction over issues of airline competition, which includes mergers and acquisitions. The U.S. Department of Transportation (DOT) exercises regulatory authority over international routes, and international tariffs and pricing, although domestic air transportation is unrestricted.

Authority to operate international routes is regulated by the DOT and by the foreign governments involved. International routes are also subject to the approval of the President for conformance with national defense and foreign policy objectives.

The DOT and certain foreign governments regulate the operations of CRS vendors. The DOT is also concerned with certain other consumer-related matters such as advertising, compensation for those who are denied boarding, baggage liability, and smoking aboard aircraft.

Many other interrelationships exist in the airline industry. The U.S. Postal Service has authority over the transportation of mail. The Communications Act of 1934 governs Delta's use and operation of radio facilities. The Railway Labor Act governs labor relations in the airline industry. Environmental matters (including noise pollution) are regulated by various federal, state, and local governmental entities.

In addition, other macro structures besides government regulation had been developed as a way to coordinate flying arrangements and collectively deal with other common issues for mutual benefit. *How did these relationships affect Y2K solutions?*

Industry relationships [93]

> [O]ur long standing relationships have been proven to work – not just on paper but in the real world of day-to-day, airport-to-airport travel (Mullin, quoted in Delta Air Lines, 2000).

Mullin had learned a lot about the air transportation sector in a short time because of dealing with the crisis of *Y2K*. Along the way, he was able also to take a leadership position to help with issues in the air transportation sector.

---

[93] Much of the material in this section regarding industry structures from Delta Air Lines, (1997). See also Appendices D & E.

Code-sharing arrangements and airline alliances

Code-sharing arrangements and airline alliances had enabled Delta to leverage its ability to provide air travel services to its customers. Many U.S. carriers had increased their ability to sell transatlantic services and destinations to and beyond European cities by code sharing. Similarly, code-sharing agreements with U.S. carriers had enabled foreign carriers to obtain access to interior U.S. passenger traffic.

> Under these dual designator code sharing arrangements, Delta and the foreign carrier publish their respective airline designator codes on a single flight operation, thereby allowing Delta and the foreign carrier to provide joint service with one aircraft rather than operating separate services with two aircraft (Delta Air Lines, 2000).

Airline alliances worked differently. Alliances represented a deeper level of cooperation based in a well-established relationship history among carriers. In particular, relationships among full service airlines generally represented the same cultures, management beliefs, labor policies, and route structures. As an example, Delta joined Aeromexico, Air France, and Korean Air to launch *SkyTeam*, an international airline alliance. *SkyTeam* airlines had

> a time-tested history of code-shares and other working relationships prior to this partnership, so [the partners] know and understand each other. [Their] similar corporate cultures, matched networks, and common performance ethics mean a smoother flight for customers, right from the start (Delta Air Lines, 2000).

In an interview with Curtis Robb (2004, Apr 7) former CEO at *Delta Technology*, he said this about the industry relationships:

> Military or code-share partners – neither really constrains Delta. Delta had to drop partners based on maintenance issues. Delta and eight other airlines have global alliances, which are terrific business opportunities to maximize passenger opportunities [i.e., Air France, Mexico, Italia, Czech, KLM, South African, Continental, and Northwest (Continental and Northwest mix frequent flyer miles)].
>
> SkyTeam alliances must meet criteria of safety, technology, and customer service. (All metrics deal with safety).

Industry-owned organizations

Delta, as a part of the air transportation industry, has an extensive network of sector-based organizations that are regulative. Organizations such as the International Civil Aviation Organization (ICAO) establish global standards for flight safety among other things.

Delta works closely with the Air Transport Association (ATA), Air Transport Association – Canada (ATAC), and the International Air Transport Association (IATA). The Air Transport Association (ATA) is the U.S. airline industry's chief lobbying group, and represents the airline industry on major aviation issues before Congress, federal agencies, state legislatures and other governmental bodies. The organization promotes safety by coordinating industry and government safety programs, and serves as a focal point for industry efforts to standardize practices and enhance the efficiency of the air transport system.[94] Delta chaired the ATA Y2K Airport Sub-Committee and led the ATA Y2K supplier programs. ATA was instrumental in coordinating activities of airports. Delta had a similar relationship with the Canadian Air Transport Association (ATAC), which had its own *Y2K* committee.

Another relevant organization is the IATA, the global trade organization for air transportation, which plays an important role in harmonizing technical standards for civil aviation worldwide. Its members comprised 265 airlines—the world's leading passenger and cargo airlines among them, which represent around 94% of international scheduled air traffic. IATA members, as scheduled and non-scheduled airlines, operate commercial

[94] See http://www.airlines.org.

air services from more than 140 nations in every part of the globe.[95] Delta held one of nine seats on the IATA *Y2K* Executive Steering Committee and Mullin served as Chairman of IATA from 1999-2002. IATA membership approved the membership-wide assessment for the expansion of the industry-wide *Y2K* program.

ACI-NA was the largest of the six worldwide regions of Airports Council International (ACI), an organization of airports worldwide. Most all domestic and international airline passenger and cargo traffic in North America goes in and out of ACI-NA airports. ACI-NA promotes cooperation within the commercial civil aviation industry for exchange of ideas, information, and experiences on common airport issues. The organization is the interpreter for key airport policy and business issues to the ACI-NA membership.[96]

The following is an excerpt from an email message sent to Delta's PMO by ATA's *Y2K* director Paul Archambeault:

> ATA PO learned on Thursday that *ACI-NA Board* of Directors denied a request for funding up to $60,000 for common airport Year 2000 testing program on the grounds that it would duplicate efforts already underway (Delta archive, 061298.txt).

Further information provided to the Delta managers described progress with other entities and their activities and concerns.

> ATA requested that WCO [World Customs Organization] begin gathering *Y2K* readiness information from its members. IATA is also in contact with WCO. ATA President Hallett of WCO met with Senator Bennett (R-UT), who chairs the *Senate Select Committee on Year 2000.* Sen. Bennett indicated concerns over FAA and airports.
>
> The ATA airport matrix was expanded by FAA to include additional items provided by ACI-NA and other items (such as locally owned navaids at smaller airports).

---

95 See http://www.iata.org.

96 See http://www.aci-na.org.

> The checklist will be expanded to include three columns: one indicating that an item is related to *FAR Part 139 airport certification*; one indicating that an item is related to the movement of aircraft on the airfield but not related to Part 139; and one to indicate that an item is related to *FAR Part 107 or 108 security requirements*. Tentative FAA target for release of the letters is the week of June 22 [1998]. On action items list are Airbus, Rolls Royce, Sunstrand Corp, and Pratt & Whitney, GE engine services FAA Flight Standards; APHIS; and NWS, FAA *Y2K* testing protocols generally, host computer testing results; and the end-to-end testing plans for FAA/airline and other system interfaces.

It was with the backdrop of this Delta context that the scenario was envisioned for the Year 2000 Program, and for the different solutions among Delta's business areas. Everything about the environment of the Delta organization pointed to the idea that coercion would come into play in a number of ways as a *Y2K solution* was designed. It seemed reasonable to conclude in advance of the investigation that institutional factors would be the overriding influence on the actions in business areas; and that these contextual conditions would force solutions that were not the same and not the best. It was surprising to come to different conclusions as the investigation developed. The story continues in the next chapter with the design of the component activities of the Year 2000 Program.

Summary

Delta formed the background context within which each of the sub-unit business areas developed its *Y2K solution.* This chapter described this context, discussing the Delta organization in broad historical overview and more specifically with respect to the study period between 1997 and 2003. The overview also included a discussion of Delta's cultural and sectoral environment. The next chapter continues the development of this context by elaborating the Year 2000 Program and its component structures.

CHAPTER 6

THE YEAR 2000 PROGRAM SUPPORTED DELTA'S FUTURE VISION

> The *Y2K* issue impacts every facet of Delta Airlines. All Business Areas and Subsidiaries of the airlines [are] in some way affected by this technological problem. Every individual within the airlines will be in some way affected by the *Y2K* issue. Coping with the *Y2K* issue will require organization wide focus and resources in order to meet the finite deadline of the year 2000 (Delta archive, "Mission Year 2000 Master Plan, Section 1.0 Executive Summary," 1998, p. 4).

> Some of you have made mention of this being the first time business, support and operating units have come together to formally discuss the business processes and the impact decisions have throughout the company (Delta archive, McCullough letter, ITcosts.doc).

> Delta Technology had to inventory, inspect, repair or replace every computer system in the company. This was a golden opportunity to upgrade where necessary, eliminate old or redundant systems, and generally produce a slimmer, *more robust* computing environment (Delta archive, Taylor, quoted in Corporate Communications *Y2K*-Normal.doc).

The aim of this case study was to understand how a complex organization like Delta addressed and solved an IT problem that affected the security of its computer-based systems. The study focused on the crisis of *Y2K*, and on the effects of context on solution choices for eliminating the *Y2K* bug. Toward this end, Chapter 5 presented an overview description of Delta, which served as the context within which each sub-unit business area developed and implemented its *Y2K solution*. The study proceeds in this chapter to bring to light the context provided by the Year 2000 Program, i.e., the *structured process* that was used to assess Delta's IT systems and to devise and implement its treatment plans. The "Future Vision" for Delta's systems that had been devised in earlier years drove this activity in large part.

Back as far as the early 1990s, Delta had identified a "Future Vision" of the ideal IT systems that would best serve the complexity of the enterprise. The vision supported management of the organizational complexity with a high level of real-time functional interdependence among Delta's IT systems, including reservations, flight planning, passenger check-in, cargo loading, aircraft maintenance, crew scheduling, etc. The vision identified the architecture along with the kinds of systems that would be needed, and the technical expertise that would be required to develop and implement them.[97] For Delta, bringing this vision to reality meant a complete transformation of its existing systems. One might therefore speculate that because of the scale and scope of such an effort, and for any number of other reasons, the Future Vision idea (along with addressing the issues with IT) had been low priority. The *Y2K bug* gave the company a reason to bring these projects to the forefront.

However, making plans to change the condition of the systems did not come without trepidation on the part of executive management. Mullin (2004) described a conversation he had with Feld in September of 1997, shortly after Mullin arrived.

> Charlie said that IT at Delta was 'abysmal.' He said Delta could not be compliant by year 2000. I called my wife, who was still in Chicago, and told her not to sell the house. I wasn't sure I wanted to take over with this facing the company.

Grinstein (Delta's Non-executive Chairman) must have offered Mullin a deal he could not refuse, since he did stay on the job. Further, he not only took on the *Y2K* project, but he led the company to apply their IT systems to garner benefits for Delta that no CEO before Mullin had been able to imagine.

---

[97] These ideas were based on ideas of the "Airport of the Future," (See NASA: http://ffc.arc.nasa.gov/).

Fortunately, some in the organization were already squarely confronting the *Y2K* problem before Mullin arrived; the methodology with all of the details outlined to complete the project had been acquired and put in place. The methodology provided a template for the project, the structure of which consisted of multiple components that cut across the four functional areas of the organization. The methodology also defined the means for coordination across the components. However, Mullin first had to engage the leadership for carrying it out. This chapter presents a discussion of the IT transformation and brief descriptions of the methodological components of the Year 2000 Program. The chapter also describes *Y2K*-related activities of organizations in Delta's external sectoral environment.

Delta's IT transformation

A number of accounts have described the Year 2000 Program at Delta as an "IT Transformation." The term "transformation" as it relates to the Year 2000 Program pertains to both the organizational restructuring within *Delta Technology*, and the changes to Delta's IT systems—to the systems architecture and to the means for user interaction. These two processes, (1) changes to organization and (2) changes to information technology, worked in tandem as equally important aspects that contributed to the favorable results that the organizations of Delta and *Delta Technology* achieved together while solving the *Y2K* problem.

Organization restructuring

The organizational restructuring began with new leadership for *Delta Technology*. After prior missteps and false starts including the failed *TransQuest* partnership and unproductive engagement of consultants, Delta finally found the leadership both for the

enterprise and for the IT organization that would produce the needed results. One of Mullin's first actions after taking the reins as CEO was to hire Feld to act as Delta's Chief Information Officer (CIO), and *Delta Technology*'s CEO.

Immediately prior to the Delta assignment Feld had served as acting CIO at Burlington Northern Inc. (BNI), the railroad company where Grinstein had been Chairman and CEO. At BNI, Feld led the integration of IT systems after BNI acquired Santa Fe Pacific Corp. The 22-month effort involved more than 60 million lines of legacy code. The real-time integrated system went live in July 1997, and Delta hired him a month later. Of note, the Delta assignment would involve installing a real-time integrated system, about 50 million lines of legacy code and had a two-year deadline.

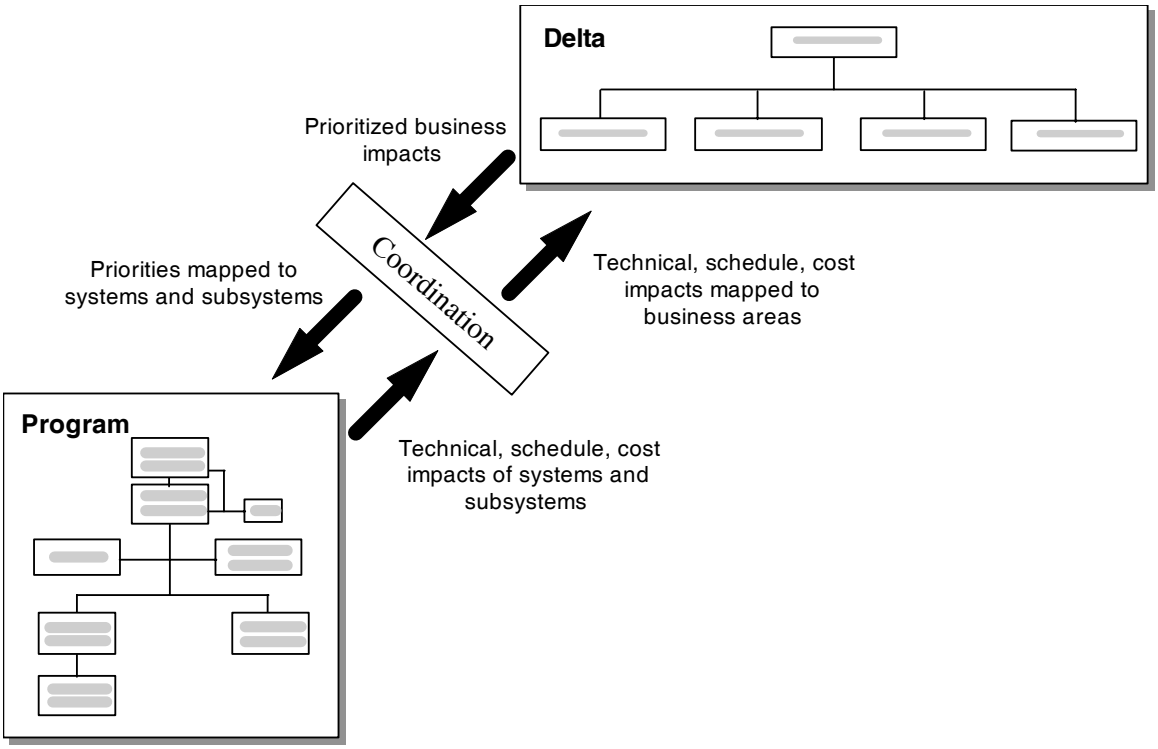
When Mullin presented the challenge of solving Delta's *Y2K* problem to Feld, he insisted that he would not take the job unless he had the freedom to transform the entire system. Feld convinced Delta's executives that his transformation approach would enable the enterprise to weather the change of millennium without incident, but more importantly, that the approach would put Delta in a leadership position in networked information systems at a time when the competition seemed to be way ahead. However, Feld did not want to take the job as a Delta employee, but rather he wanted to do the work in a consulting role. Mullin, according to Feld, was accustomed to managing a more traditional leadership team where all members were employees; but in the interest of getting Delta's IT issues put to rest, he met all of Feld's terms. Thus, Mullin gave Feld responsibility, as a consultant, for the development and operations of Delta's wholly owned subsidiary, *Delta Technology*.

When Feld first came on board, Delta's IT company was still called *TransQuest*. Feld was instrumental in changing the name of *TransQuest* to *Delta Technology*, but other changes that followed were also dramatic. The early activity following Feld's hiring involved re-mixing roles and responsibilities. One informant described it this way:

> Feld began a minor cultural revolution. He selectively moved employees to comparable responsibilities in new divisions. People became disconnected from others they were accustomed to working with. At an informal gathering after work with former co-workers, a secretary confided that Feld had requested a confidential report of how people were getting along in their new places.

During this time, Feld assessed skill levels of IT staff, began a process of firing and hiring, identifying leadership and processes, reorganizing for *Y2K*, and outsourcing code cleaning. Feld commented on the pace of work during the project initiation, "… coming off of failed outsourcing and a lot of junk, we worked in 90 day increments" (Feld, 2006).

With all of the changes that happened inside the *Delta Technology* organization, one thing that did *not* change was the organizational structure. During the phase of cross-populating within the organization, Feld had maintained the divisional structure of *Delta Technology* that had been established before his arrival. In the prior year, which was the inaugural year of *TransQuest*, the employees had been organized to work in teams ("portfolios") that corresponded to the business areas in Delta. This structure was based on mapping Delta's functional areas to the IT systems that supported their activities. This structure would serve to organize the Year 2000 Program. Figure 3 illustrates the Year 2000 Program coordination between the portfolio divisions in *Delta Technology* and the business areas of Delta.



Source: Delta archive, "Figure 3-3. Mapping Technical and Business Risks," 1997.

Figure 3: Year 2000 Program maps a business area onto its technology portfolio

Customer Portfolio's work in *Delta Technology* related to software applications (systems) that supported customer-interfacing functions, such as airport gate and ticket agents, in the *Airport Customer Service* business area of Delta. Airline Operations Portfolio performed systems work related to the functional activities supporting Delta's pilots, flight attendants, and mechanics in the *Operations* business area of Delta, Business Support Portfolio performed systems work for Delta's finance function, legal, HR, etc. Revenue Portfolio performed work in support of the sales and marketing groups. In contrast to the aforementioned groups, a fifth portfolio, Technology, provided infrastructure support for the other four portfolios' application software, and for the global enterprise-wide architecture systems. The Technology portfolio supported the

entire Delta enterprise, providing engineering and support services for desktop units, file/print/communication servers, networks, and system platforms. During the study period, the Technology Portfolio was divided into three groups: Common Services, Engineering, and System Operations. Common Services covered database, development tools, Intranet services, middleware services, and usability engineering. Engineering dealt with change and configuration management of IT infrastructure systems, including networks and workgroup systems. The third division, System Operations, managed platform operations, the help desk and field services. See Appendix D for a diagram of the *Delta Technology* organization structure.

The Year 2000 Program combined employees from Delta and *Delta Technology*, assuring not only that the process was not limited to the IT staff, but also that the Program included input from business people who understood the business processes that were required to run the company. At first, the Program organization had problems with leadership. Even though the methodology had been defined for running the Program, it was not until late in the spring of 1998 that the people were put into positions that allowed strong forward progress.

Organizing the Year 2000 Program

> It is imperative that Delta create an audit trail of all our Year 2000 efforts so that we can prove due diligence if we have the unfortunate experience of being involved in any Year 2000 litigation (Delta archive, "Delta's Enterprise Year 2000 Management Overview Inventory Phase," 1997, p. 2).

Methodology

The methodology for the Year 2000 Program, called SMART/2000+™, was purchased from the BDM consulting company. This methodology defined all of the

coordinating organizational and activity structures. Roles and responsibilities were defined and the activities were structured in phases. A central Project Management Office (PMO) was established to coordinate all of the *Y2K* related activities. The PMO included Program Control, Quality Assurance (QA), Configuration Management (CM), Testing & Compliance Validation, Systems Architect (SA), Risk Management, and Communications. Some areas of the PMO were difficult to fill by only a Delta team member because of the lack of expertise. BDM contractors filled some of these roles. Ten people, including a representative from legal and media relations, met every week. They dealt with coordination mechanisms prescribed by the project methodology, such as keeping records on inventory, assessments, etc. This group also managed *Y2K* issues related to entities external to Delta: fuel, FAA, airports, weather, immigration, maintenance suppliers. The group was dissolved after the year 2000 rollover.

An IT board provided oversight for strategy implementation and determined IT priorities, in addition to providing coordination among Delta IT personnel, *Delta Technology*, Worldspan, and Delta's business areas. The IT Board consisted of the CFO, the Executive Vice President for *Airport Customer Service*, the Controller, and the heads of Flight Operations, Customer Commitment, and Distribution Planning (Delta archive, Res Conference.ppt)

Table 8: Delta Information Technology (IT) Board

Paul Matsen	
Charlie Feld (executive sponsor)	
Charles Gravitt (managing director)	
Business	**Technology**
Portfolio Owners	Portfolio VPs
Portfolio Managers	Portfolio Director
Business Director	Portfolio Teams, core & extended teams

Walter Taylor directed the work of the Delta systems assessments along with the changes that had to meet the year 2000 deadline. Taylor, a military veteran and Delta pilot had a definite "command and control" attitude about the project.

> *Y2K* represented a "burning platform," and needed a battlefield military mentality (Taylor, 2004, Apr 13).

There were 600 people involved in the Year 2000 Program. A person in each business area (a "strong contributor") was assigned to Taylor. The idea was "don't remove accountability for the work – take someone out of the regular work force who knew the system, and was responsible" (Ibid.).

Table 9 shows the leadership by Portfolio. Note that Taylor was also the VP in charge of the Operations portfolio.

Table 9: Year 2000 Portfolio owners & Portfolio VPs

PORTFOLIO	DELTA OWNERS	*DELTA TECHNOLOGY* VPs
Business Support	Ed West	David Pittman
Customer	Vicki Escarra	Keith Halbert
Operations	Mac Armstrong	Walter Taylor
Revenue	Vince Caminiti	Mark Sohl

The Program was assigned "high priority" status relative to other work activities, and given liberal funding. Delta's executive management felt that due to the critical nature of the *Y2K* issue, the Program required a more flexible funding process than existed in other areas. Understanding the nature of this issue to the organization, Mullin's attitude was to invest whatever was necessary to get the job done.

> [Delta] utilizes software and related computer technologies essential to its operations that will be affected by the Year 2000 issue. Delta is studying what actions will be necessary to make its computer systems Year 2000 compliant. The expense associated with these actions cannot presently be determined, but could be material (Delta Air Lines, 1997).

The SMART/2000+™ plan called for seven phases: Awareness, Inventory, Assessment, Migration Planning, Renovation, Testing/Validation, and Implementation/Integration. Table 10 shows some of the Delta events during the Inventory, Assessment, and Treatment phases. These phases were roughly defined; and the dates are somewhat different in various documents.

Table 10: Year 2000 team activities by Program phase

INVENTORY PHASE	SEP 1997-FEB 1998
Conduct a physical inventory of all business area/enterprise assets.	
Attend Atlanta *Y2K* Users Group	08-25-97
BDM consultants helped to implement Delta Enterprise PMSR process for the Core Team and Extended Team meetings.	09-11-97
Core team complete	09-15-97
BDM support for configuration mgmt (CM)	09-29-97
Ensure *TransQuest* backup and recovery systems are sufficient for the *Y2K* data (PMSRs and database)	10-20-97
Decision not to use Clearcase or Documentum for CM	01-28-98
ASSESSMENT PHASE	FEB 1998-JUN 1998
Assess *Y2K* readiness, risk in IT equipment and systems, non-IT equipment, and facilities. Assign criticality as high, medium, or low. If approved, *Y2K* assessment of low criticality items may be deferred to the Treatment Phase. However, low criticality items will be completely assessed no later than 12/1/98. Determine estimated date for completion of external suppliers' *Y2K* programs. [98]	
E&Y leading coordination between *Delta Technology* and Suppliers.	03-02-98
Charles Gravitt of *Delta Technology* assumes the position of Managing Director with four full-time Directors in the areas of Remediation, Testing, Knowledge Management, and Business (non-IT).	03-23-98
TREATMENT PHASE	MAR 1998-JUN 1999
Take corrective measures to assure equipment, systems, and facilities are capable of processing data with date sensitive fields before, during, and beyond the year 2000. This includes developing business continuity plans. For external suppliers, the phase evaluates supplier progress against stated *Y2K* plans.	
Meet with connection carriers to discuss *Y2K* status & readiness of regional airports.	07-09-98
Determine assessment and compliance validation procedure for aircraft certification.	07-14-98
Determine level of detailed information we can obtain from ATA/IATA that supports readiness of an airport, supplier, and regulatory agency.	09-25-98
Coordinate and engage int'l station managers with *Y2K* (IATA effort and efforts within their airports).	10-30-98
Identify contact and create process for remediation of bag and mail sortation systems.	11-03-98
Meeting with FAA, Delta's Mac Armstrong attends.	01-20-99
ARINC begins testing, sends list of all services ARINC provides to Delta.	02-01-99

The Inventory and Assessment phases provided the foundation for the remaining phases. The assessment phase provided more detail as to the nature of the systems for

[98] These strategies are addressed in Delta archive, "Year 2000 correspondence E-GDTS-1606-006.00."

which the teams were responsible. Table 11 shows the breakdown of the *Delta Technology* portfolios according to numbers of systems and total lines of code (LOC) that required assessment and possibly "cleaning" to eradicate the *Y2K* bug.

Table 11: Distribution of systems by *Delta Technology* portfolio

PORTFOLIO DIVISIONS	# SYSTEMS	LOC (MILLIONS)
Application portfolio		
Business Support	111	11.2
Customer	35	2.8
Revenue	14	10.2
Airline Operations		
Flight Operations (Flight Ops)	35	8.5
Technical Operations (Tech Ops)	36	15.9
TOTAL	**231**	**48.7**
Technology Portfolio		
Common Services		
Database	92	
Development Tools	267	
Intranet Services	15	
Middleware Services	48	
Usability Engineering	47	
Engineering		
Large Tier Engineering	230	
Mid Tier Engineering	233	
All Unix Servers	610	
Network Engineering	231	
Systems Management	70	
Workgroup Engineering	575	
System Operations		
Field Services	191	
Platform Operations	20	
ENTERPRISE TOTALS	**2250**	

Source: Delta archive, EC Update0399.ppt.

The objectives for Year 2000 date compliance were defined, the source code from the Inventory phase was extracted and sent to the BDM renovation center, the code was scanned for Year 2000 date issues, and reports showing the results for each subsystem were generated. The idea was not only to determine the scope of the project, but also to

prioritize activities by how critical the systems were to the airline and how difficult each would be to remediate.

Each computer-based system was assigned a criticality level based on the following guideline (Delta archive, Workshop Presentation.ppt):

- High - Failure that could affect safety or result in costs that are potentially fatal to the organization … can't provide service which is our business.
- Medium - Failure that could result in substantial but not lethal costs to the organization … systems without which we lose our competitive edge.
- Low - Failure that could result in trivial costs or only an inconvenience to the organization ... systems which make us efficient and more productive.

The primary scanning tool used in the analyses varied with programming language. The Formal Systems and Insight 2000 scanning tools were used to scan Natural language code. The Cap-Gemini tools scanned source code for COBOL, Client Server, and other languages. Following the date analysis, if a subsystem met any of the criteria listed below a waiver from the assessment process was granted to that application.

- The application was already Year 2000 compliant
- The application did not contain any date issues.
- The application was to be retired prior to its projected failure date.
- The application was to be replaced with a Year 2000 compliant system prior to its projected failure date.

The result of the scanning process would be classification of a system as waivered (*Y2K* compliant), or as candidate for some level of treatment regarding the *Y2K* bug. The code was also assigned a rating (HIGH, MED, or LOW) that indicated the difficulty of renovation based on scan information (Delta archive, ASR_123197 Lang-LOC stats 12.97.doc). The details of this information played a key role in the Migration Planning phase (*Y2K solution* design process) where it was used to assist in determining the requirements for personnel and other resources, as well as cost estimates for achieving

Year 2000 readiness. The process for designing a detailed solution for Y2K (Delta archive, OPS Migration plan 04.98.ppt):

- Direction for each application
- Complexities
- Enhancements
- Grouping and sequencing
- Cost Estimates

By January 1998, Human Resources had augmented Delta's key Leadership Performance Assessment (LPA) criteria to include integration of Year 2000 objectives (Delta archive, ACT_ITMS.xls, 1999).

Year 2000 Program implementation

The Year 2000 Program implementation encompassed several component activities operating concurrently. These components are referred to in this dissertation as "business area" activities and "infrastructure" activities.[99] Business area activities relate to changes in specialized software systems for users in particular functional groupings of core business areas such as the finance function, aircraft maintenance, customer-related activities, etc. Business area activities are further described in Chapter 7 as individual sub-cases. Infrastructure activities relate to changes in the infrastructure framework of support and services for IT operation that was shared by all users across the organization, and are described in the next sections.[100]

---

[99] The *Delta Technology* organization included five portfolio divisions: Customer, Air Operations, Business Support, Revenue, and Technology. For purposes of this research, in order to distinguish functional business area activities from infrastructure activities, the four Portfolio divisions are called "business areas," and the Technology division, "infrastructure."

[100] Infrastructure may also be related to services that extend to external entities.

Infrastructure activities: enterprise-wide changes to IT systems

The infrastructure project began in 1998 and (including the other portfolio work), by year 2003 had cost $1.6 Billion, according to Robb.[101] The objective of the Year 2000 Program involved changes to computer-based systems; but the changes that Delta envisioned involved more than changes to date codes. During the first year of *TransQuest*'s operations, 1995, the future vision for computing had been defined whereby major restructuring of Delta's computing architecture would enable real-time information processing. The emergency nature of the *Y2K* bug simply gave the company a reason to accomplish it more quickly.

Delta's essential IT processing was based in mainframe computers and servers that served as central sources for electronic data storage, computation, and information retrieval and delivery for all of Delta's business area users.[102] Desktop units comprised 36,000 standalone computers and 12,000 "dumb terminals"[103] that were located at various business area sites across the Delta organization. Each desktop unit interacted with the mainframes via operating system software and application software systems. However, many of these software components controlled functions that were unique and were available only to serve the needs of users in a particular business area. The output of these systems was confined to the business areas where they had been developed.

---

101 See also: "Staying the Course" (2003).

102 Delta operated 4 IBM 2064s mainframe computers with 21 CPUs in the RCC, and 3 more IBM 2064s with 17 CPUs in the ACC. In addition, Delta operated 1,441 Intel-based servers, and 750 Unix servers, 350 Sun and 400 HP. Worldspan operated 9 IBM 9672s in the RCC that were dedicated to Delta production, and 9 more in the ACC that were dedicated to Delta disaster recovery.

103 A dumb terminal is a unit that has a monitor and a keyboard, but no generalized processing capability on its own. It is limited to input of data to (and display of output from) another computer as host (historically a mainframe).

Delta Nervous System

> Seeking to avert a *Y2K* crisis, Delta invested $1 billion in its IT infrastructure and developed a publish-and-subscribe environment to support a cross-functional customer-orientation (Ross, 2001).

During the Year 2000 Program, *Delta Technology* developed and implemented new system infrastructure. Operating within this new IT environment had resulted in increased productivity and efficiency across the company. A bottom-up approach was used to develop it, where all the business areas were evaluated separately. Each new application component was designed to serve the needs of each business area. Table 12 shows the new system components.

Table 12: Delta Nervous System (DNS) components

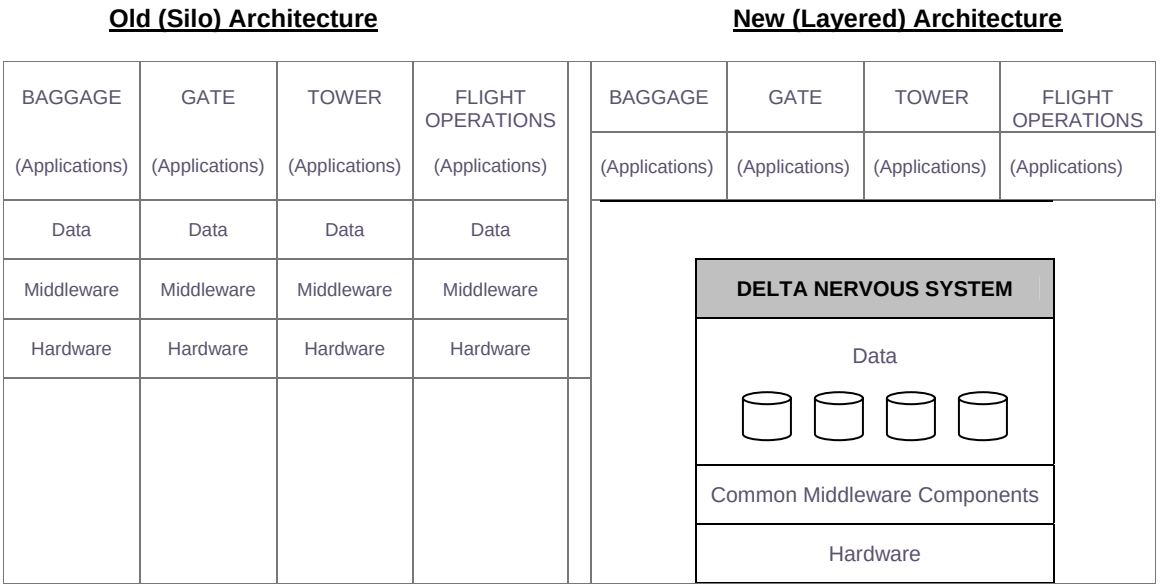
APPLICATION	PRODUCT	SUPPLIER
Delta Nervous System	Active Enterprise suite, including Active Portal and Active Exchange	Tibco
Messaging software	Rendezvous, MQSeries	Tibco, IBM
Data warehouse	Teradata	NCR Teradata
Databases	Oracle, DB2	Oracle, IBM
Systems management	OpenView, HP	Tivoli, IBM
Transaction processing	Tuxedo, CICS, BPM/InConcert	BEA, IBM, Tibco
WEB SITE		
Application server	WebLogic	BEA Systems
Content Management	Enterprise Content Management Platform	Documentum
HARDWARE		
Delta runs many of its applications on Hewlett-Packard HP 9000 Series servers and HP Vectra PCs		

Source: Gage & McCormick (2003).

Delta named its new infrastructure system the "Delta Nervous System" (DNS), a digital network designed to receive continuous data input, then store it, organize it, filter it, and / or report it to the organization. One of the attractive attributes of the infrastructure design benefiting the Year 2000 Program was that the DNS used middleware to defer or to bypass dealing with legacy systems. The design of the system was similar to the development of the original Internet, not overly complex, not disruptive of existing

responsibilities and power relationships, and therefore not contributing uncertainty (Ker, 1994).[104]

The DNS functioned as a series of layers, so that services were decoupled from the infrastructure; and new services could be added without necessitating changes that would disrupt the structures and integrity of the legacy systems. Figure 4 is a simplified diagram of the old and the new IT architecture.



Source: Feld & Stoddard (2004).

Figure 4: Old vs. new (DNS) system architecture

The DNS linked all of Delta's IT functions into two databases: a real-time operational database and a data warehouse for performing analysis and producing reports. Data-management vendor Teradata then worked with *Delta Technology* to create the

[104] In developing the Internet, a "black box" served as an interface, so that each organization's computer system could connect to it for communication with other locations without changing its core functions. See Abbate (1999).

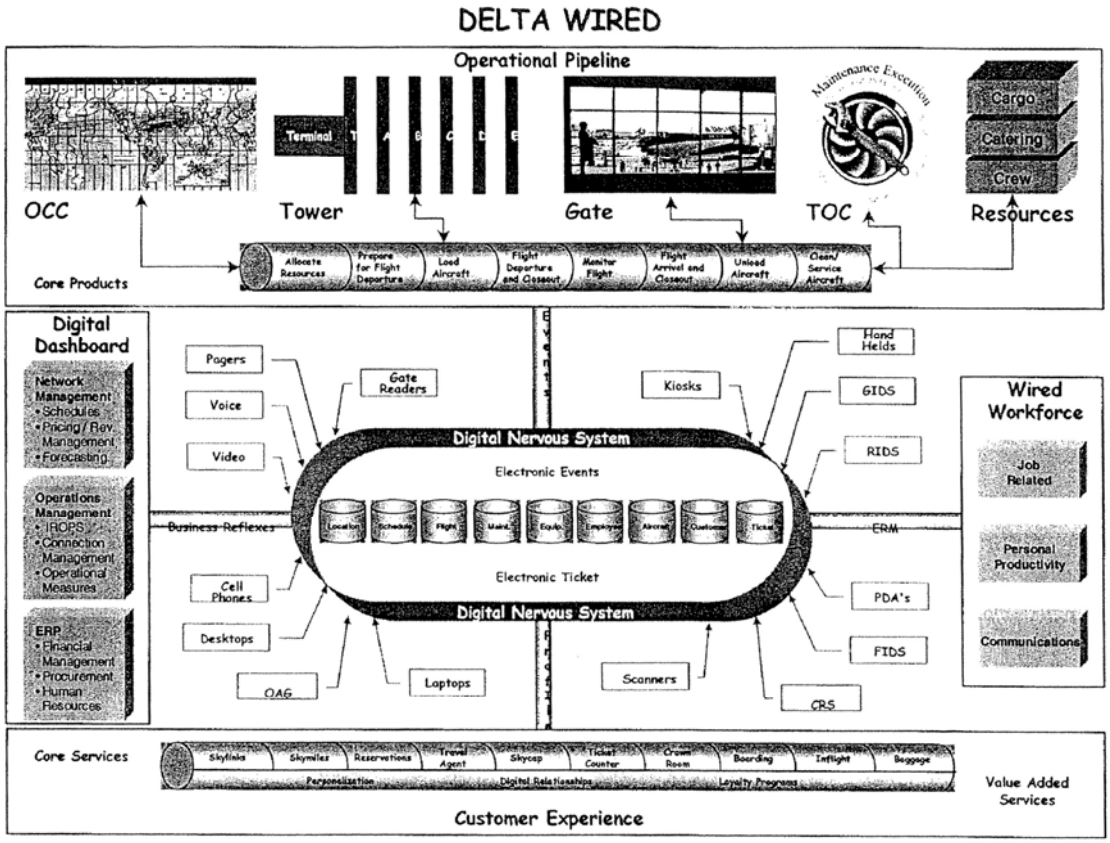
cross-enterprise data repository that was fed by a number of business area systems. The information required for the core processing was stored in nine centralized "datastores":

- Inventory Management
- Revenue
- Fares & Pricing
- Schedules Reengineering
- TOC Maintenance
- Sales & Distribution
- Operations Control Center
- *Airport Customer Service*
- Customer
- Tower / ACC (Airport Coordination Center)
- In-Flight

A representative of the database vendor said,

> Delta has the most comprehensive data warehouse in the airline industry … most airlines get about 20% of their transactions into a data warehouse. At Delta … almost every transaction is in there (Elsworthy, quoted in Gage & McCormick, 2003).

Middleware was built around the databases so that new applications could access and update the data. This architecture allowed deferring decisions to install new or later models of software. The entire Delta enterprise system is depicted in Figure 4.



Source: Ross (2001).

Figure 5: Delta IT system enterprise-wide

> The system is not finished. In the works are more customer-facing applications, operations and revenue management functions and—a new need—security. But the result so far is stunning, creating efficiencies that have pushed Delta's workload cost far below its competitors and not far above a theoretical minimum, according to a Gartner IT assessment. With DNS, Delta clearly established its technology leadership credentials (Technology Leadership: Delta Technology, 2004).

Code remediation

> The productivity gains from the Ukraine Off-Shore Support Team, which are proving to be substantial, will not be factored into these estimates (Delta archive, ASR_123197 Lang-LOC stats 12.97.doc).

For those elements determined to be non-compliant (not *Y2K* ready) in the assessment phase, some form of remediation was required. Remediation meant bringing non-ready systems to a ready or compliant state. Targeted first toward critical systems,

options existed for standard remediation. For those items and systems found to be not ready, a business area could elect to remove them from use and replace or upgrade as necessary, or to renovate. Decisions on which option to choose were based on the following factors:

- Criticality
- Item Life Expectancy
- Cost to Replace Versus Upgrade
- Future Plans
- Present Use
- Operational Impacts

If an upgrade of the equipment or product was available, this was usually the most expedient cost-effective approach and generally had less of an impact on operations than replacement. Renovation of the equipment or product was typically reserved for those situations where the non-compliant element was no longer supported by its vendor or had been developed in-house. A *Technology Review Board* was created to resolve any migration planning issues that could not be resolved by the individual Portfolio Coordinators (Delta archive, OPS Migration Plan 04.98.ppt). Figure 6 shows the cost approval and spending process to support these decisions.

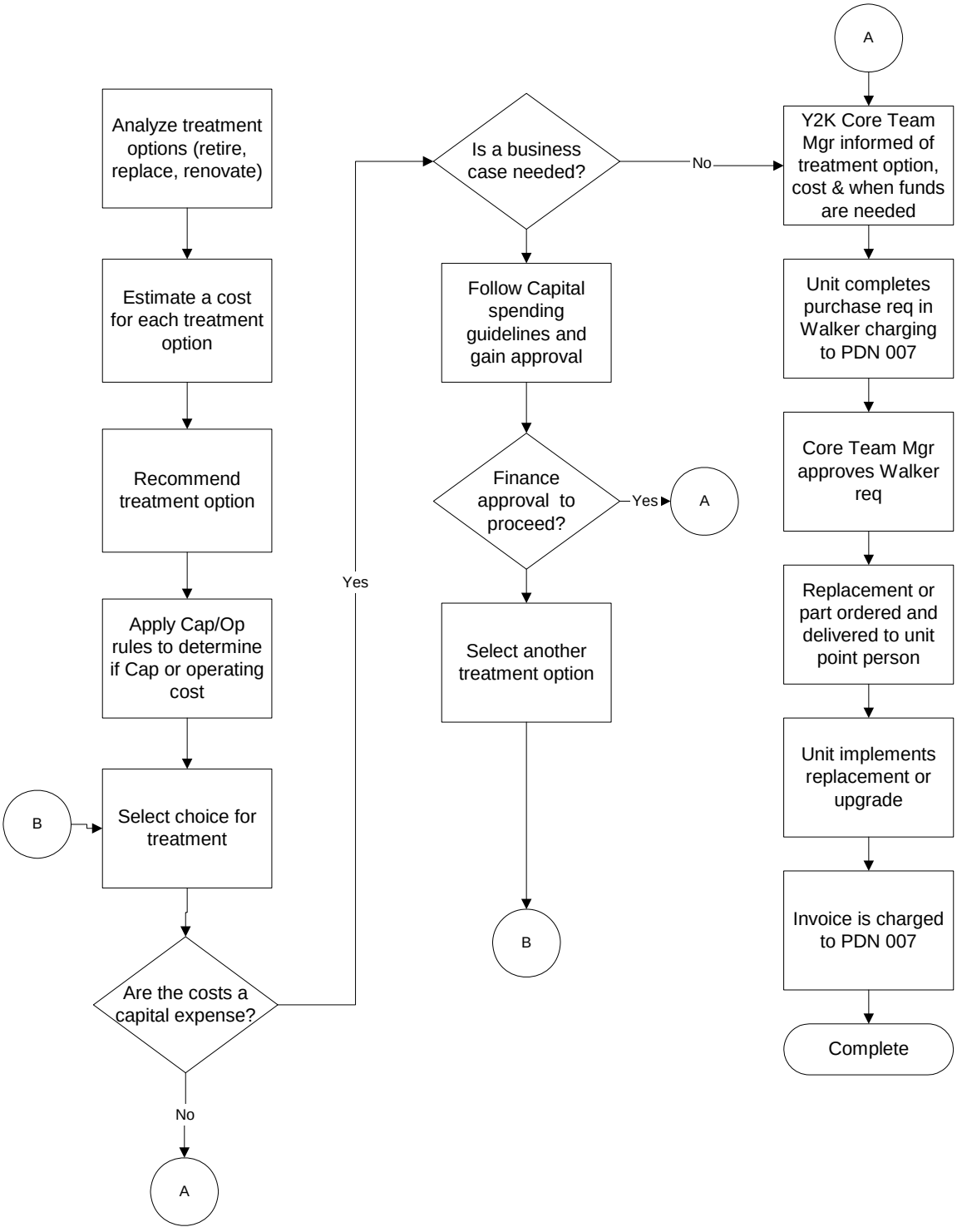


Figure 6: Cost approval and spending process for the Year 2000 Program

Requirements for code remediation were established by the business area teams. Actual accomplishment of remediation for Delta involved outsourcing.

> We did in-house remediation as well as off-shore. Off-shore (AG software & others) didn't work well because they didn't understand the systems. However, Delta used them to verify remediated code. They couldn't verify it, but could red flag possibilities. Delta could then double-check (Taylor, 2004, Apr 13).

About 90% of the code was sent to a consulting company in Kiev, Ukraine, while the other 10% was sent to Software AG, a German software company that had developed the Natural programming language. The cultural aspects of the code remediation project were interesting: Delta's connections with the Ukraine consultants, its management by an employee relatively new to Delta, and the overt recognition of information security—rare in other aspects of the Year 2000 Program.

Delta's connection to The Institute, a consulting company in Ukraine, came via the U.S. State Department. Neal Morgan, who provided the leadership for code remediation had been recruited in 1996 from outside the company. As a retired military officer, he had extensive experience not only in IT, but also with the setting of IT in Eastern Europe. *Delta Technology* employee Eugene Shtern provided liaison with The Institute, as he was a Ukraine native. These two employees traveled to Kiev part of every week for over a year to facilitate the code remediation project. The project was reported to have saved Delta $12 million over what it would have cost if a U.S. consulting company had performed the work (Shtern, 2007).

Concurrent with the *Y2K* design and development activities were the Desktop Strategy Project and the Renewal projects, which were groups who worked to design and to implement, respectively, the hardware and software solutions enterprise-wide.

Desktop Strategy Project

The Desktop Strategy Project represented aspects of both infrastructure and specialized software (business area) systems in the Delta organization. Desktop units

represented infrastructure components that were common to all users, but desktop units also comprised software systems that varied by business area. Therefore, because of the enormous variety in the components of the units enterprise-wide, Delta strategists decided that inventory of the units was most efficiently accomplished autonomously by business area end-users. Table 13 shows the roles and assignments for the Desktop Strategy Project.

Table 13: Desktop Strategy Project personnel assignments by business area

ROLE	***BUSINESS SUPPORT***	***AIRPORT CUSTOMER SERVICE***	***OPERATIONS***	***REVENUE***
Delta VP	Ed Bastian	Vicki Escarra	Jenny Poole	Vince Caminiti
Delta Mgmt Sponsor	Sharon Moody	Robin Stricklin	Tim Rider	Larry Beck
Delta Technology Mgmt Sponsor	Fred Collins	John Jacobi	Mark Hicks David McGlothlin	Steve Smith
Delta Coordinator	Phil Stanley	Liz Boothe (RES) Timothy Johnson (Dist. Planning) Pat Roberts (Consumer Mktng) Daiquiri Gleaves (Consumer Affairs)	Doug Breed (Airline Ops) Peggy Reagan (Tech Ops) David Nagelhout	Keith Drewski
Delta Technology Coordinator	Rip Dickinson	Kevin Hutcheson	Theresa Ryan	Steve Cooper
Desktop Lead	Joel Ellis (10/'98)	Melanee Haywood	Vernon Fulton	Fran Rutledge
WGE Coordinator	Kirk Rice Jason Adams	Ken Ward Lisa Peters	Bic Vogel Jack Uys	Ginger Gouveia Vera James
FSVC Coordinator	Susan Marchant	Bill Jeffrey	Susan Ross	Susan Marchant
Delta Desktop SME	Assigned JIT by DAL Coordinator	Assigned JIT by DAL Coordinator	Assigned JIT by DAL Coordinator	Assigned JIT by DAL Coordinator
Delta Technology Desktop SME	Assigned JIT by *Delta Technology* Coordinator.	Assigned JIT by *Delta Technology* Coordinator.	Assigned JIT by *Delta Technology* Coordinator.	Assigned JIT by *Delta Technology* Coordinator.
Renewal Desktop Coordinators		Airport: Bryan Lamberth Campus: Majid Mohseni Reservations: John Jacobi Tech Ops: Bryan Price		

"The Year 2000 Desktop Strategy Project was one of the multiple components of the IT overhaul. Prior to the renewal effort, almost every desktop was unique" (Mitchell,

2006, Feb 21). The *Y2K solution* was to replace vs. patch these systems in every place where it was possible to do so.

> Delta Technology Workgroup Engineering has recently determined that most desktop computers in use at Delta Air Lines are not Year 2000 compliant. This includes the hardware and most all desktop operating systems …. Considering that there are approximately 25,000+ desktop computers in use at over 300 locations the challenge is significant (Delta archive, "*Y2K* Desktop Charter," 1998).

The project approach included identification and evaluation of existing desktop computing models for each business area within a portfolio. A computing model described a set of desktop computers that shared the same hardware and software configurations. Following the identification and evaluation process, a solution model was developed for each computing model to ensure Year 2000 compliance of each component. Compliance was attained either through the recommended Future Vision model upgrade, or by a secondary recommendation that included software and/or hardware patches. The Desktop Strategy Project was responsible for Planning, Analysis, and Design as follows:

- Define current state of desktops in each Portfolio
- Determine Year 2000 issues
- Develop appropriate Renovation Strategy

The Renewal Projects were responsible for

- Implementation Planning
- Implementation

The Future Vision desktop model was a set of hardware and software systems designed to standardize desktop units as much as possible across the Delta organization, but configured where necessary to accommodate specialized requirements of processing

in a business area, and in some cases for a specific user. Each model was designed around the following set of standard attributes:

- Hardware
- Operating System
- Network Operation System
- Delta Application
- *Delta Technology* Applications
- Estimated # of Clients
- Estimated # of Locations

The Future Vision model (Table 14) was a configuration model for desktop units. The benefit of this standardization was stated to be "reduction of technology footprint" (Delta archive, BA Review.doc). Vendors that were considered for supplying the replacement hardware included Dell, Gateway 2000, Hewlett Packard, IBM, NCR, Toshiba, and Westinghouse. The project team would recommend migration to the standard model where possible.

To expedite the assessment of desktop units with respect to the *Y2K* vulnerability and their criticality to the business area, the project required the skills of infrastructure experts, business area systems specialists, as well as business area users. Decision-making concerning the renewal or replacement of systems was accomplished at the business area level. Year 2000 decisions either to replace systems or patch, even though the preferred option of CIO Feld was to replace. Feld had noted that, "the Atlanta airport alone had over 6000 desktops in it" (Feld, 2006).

The Desktop Strategy Project strategy was to inventory and assess existing desktop computing models for each sub-organization within a business area. The project

team would then develop an appropriate renovation and implementation strategy, which would include, where possible, recommending migration to the standard model.

Table 14: Standard Future Vision model for desktop units

5: ELECTIVES			
discretionary software			
4: BUSINESS AREA SUITES			
BUSINESS SUPPORT FOUNDATION ACS – BACKOFFICE, ETC.	*CUSTOMER* PUBLIC CONTACT RESERVATIONS CAMPUS, ETC.	*OPERATIONS* IN-FLIGHT OCC, SAFETY, ETC.	*REVENUE* PASSENGER SALES REVENUE ACCT., ETC.
3: ENTERPRISE COMPONENTS			
Common Services Emulators - DLTN3270, DLTerm32, VECTR32 Middleware Database Development Tools	CS Add-In's Extra! Kea!X MS Project Visio BRIO LANYON Etc.	Workgroup Office Pro Outlook Internet Explorer Acrobat	
2: GROUND ZERO COMPONENTS			
Operating System MS Windows NT 4.0 (Desktop)	Systems Management Tivoli HP Top Tools	Information Security Norton Anti Virus MSGINA	
1: HARDWARE COMPONENTS			
Desktop HP VECTRA VL8, Pentium III, 450 MHz, 128MB RAM, 10.1 GB Hard Drive, 32X CD-ROM			

Source: Delta archive, "*Y2K* Desktop charter," 1998.

The Desktop Strategy Project was one of the Year 2000 Program groups that provided direction for the renewal groups. The scope of the project included providing the process, management, and oversight to ensure that all desktop units were renovated, but the actual implementation would be done by the renewal groups.

Renewal groups

Multiple renewal efforts across the Delta organization targeted upgrading the technology infrastructure to Future Vision standards (Ibid.):

- Airport Renewal
- Tech Ops Renewal (Maintenance renewal)
- Reservations Renewal (*Airport Customer Service*)
- Headquarters Campus Renewal
- Sales Force Renewal

Table 15 provides "snapshots" of the goals and conditions of Delta's IT systems as of 1997 and 2003.

Table 15: Snapshots of Delta IT, 1997 & 2003

TRANSQUEST 1997	*DELTA TECHNOLOGY* 2003
Business goals:	Business goals:
• Improve IT response to Delta's business needs • Cut IT costs • Market industry-specific applications	• Serve Delta's business needs • Create efficiencies in enterprise-wide business processes
Applications:	Applications:
700 total	382 in-house 599 COTS/system software
Workstations:	Workstations:
25,000 HP Vectra and Dell PCs 11,000 dumb terminals	36,000 HP Vectra PCs 1,000 Unix terminals 11,000 Westinghouse terminals 845 kiosks
Servers:	Servers:
900 Intel-based 175 midrange and enterprise Unix, primarily NCR (some Sun and HP)	1,411 Intel-based 750 Unix (350 Sun, 400 HP) 108 dedicated email servers
Mainframes:	Mainframes:
2 Hitachi Skylines 4 IBM 3090s	7 IBM 2064s
Operating systems:	Operating systems:
Migrating to Unix or Windows NT on servers and to Windows NT 4.0 or Windows 95 on workstations	Unix or Windows NT on servers Windows NT 4.0 or Windows 95 on workstations
Databases:	Databases:
Migrating to Oracle	Oracle
Network connectivity:	Network connectivity:
LANs: FDDI, Ethernet or token-ring	LAN interconnect network: standards-based, high-speed LAN/WAN environment: routers, switches and hubs, ATM, ALC, voice and frame-relay circuits, TCP/IP protocol, wireless access points.
Systems/network management:	Systems/network management:
Tivoli TME-10 and HP OpenView	Tivoli TME-10 and HP OpenView

Source: various, including Caldwell (1997), "Delta Technology Fun Facts" (2003).

Table 16 provides a brief chronology of events related to the Year 2000 Program. The next section describes some of the activities in the air transportation sector.

Table 16: Chronology of events in the Year 2000 Program

DATE	EVENT
Dec 1995	Work on *Y2K* begins at Worldspan
Oct 1996	Year 2000 Program kick-off at *TransQuest*
Jul 1997	Year 2000 Program announced to Delta employees
Aug 1997	Leo Mullin hired as CEO
	Mullin hires Charlie Feld and The Feld Group
Dec 1997	ATA begins to coordinate *Y2K* activities in the air transportation industry
Mid 1998	DNS infrastructure project begins
Sep 1998	Desktop Strategy Project kickoff
Sep 1998	Installed the CustomerCare prototype at Delta's facility in the Jacksonville, FL airport.
Jun 1999	Deployed the CustomerCare application in four major U.S. airports.
Jan 2000	Delta announced *Y2K* success
after rollover	Work begins on applications deferred before the rollover

Y2K activities in the air transportation sector [105]

> Since the fall of 1996, Delta pursued sound technology solutions and shared its knowledge with the airline industry in efforts to assist other airlines, airports, vendors, and suppliers in achieving Year 2000 readiness (Delta archive, Y2K-Normal.doc).
>
> With over 20 ATA member airlines solving the same problems with the same suppliers at the same airports, it is easy to predict a disaster is in the making. We firmly believe we [i.e., Delta] can achieve our goal of higher quality preparedness, lower *Y2K* costs and improved consumer confidence through working together (Delta archive, BODDec97.doc).
>
> $8.8 - 9.0 million. Elements: increase of ATA staff by 2.5 FTEs; 42 FTE airline representatives; outside consultant increased for airport evaluation. Delta share: Maximum of $1.6 million plus 7 FTEs for at least nine months (Delta archive, BODMar98.doc).

Air transportation organizations determined that many external suppliers were common to all members of the industry group. Therefore assessing in one place the preparedness of these suppliers optimized resources used for *Y2K* activities. Organizing

[105] Most of this section from Delta archive, "Y2K Program Overview Facts."

and performing these processes on behalf of numbers of entities reduced redundant inquiries and costs. Since airports were one of the common denominators, the FAA and a number of aircraft parts suppliers formed a *Y2K* industry team through the ATA. This team consisted of ATA member airlines and cargo carriers, and their purchasing departments. Delta adopted "conformity requirements" for these processes from several sources including the British Standards Institution.

Delta CEO Mullin was active as a member of the Board of the Air Transport Association of America and a member of the Board and Chairman-designate of the International Air Transport Association in 1999. He was also a member of The Business Council, The Business Roundtable, and the President's Export Council, all prestigious groups populated by leaders of the major infrastructure organizations in the U.S. and places where *Y2K* policy and procedures were discussed. Feld and Taylor represented Delta at Senate hearings regarding *Y2K*.

Government

FAA

> The FAA promotes aviation safety in the interest of the American public by regulating and overseeing the civil aviation industry to make sure that the United States is operating a safe aviation industry (http://www.faa.gov/).

As an agency of the U.S. federal government, the FAA had authority to promote safety and to combat aviation hazards. The FAA had sole responsibility for developing and maintaining a common civil-military system of air navigation and air traffic control (ATC). The FAA was also responsible for pilot and aircraft certification, safety rulemaking and enforcement, and airway development. The FAA was one of several organizations within the DOT, a cabinet department created by Congress in 1966.

Since the Federal Aviation Act of 1958 created the FAA, the agency had assumed responsibilities over time beyond what the law originally designed. The FAA had become involved in the field of aviation security during the hijacking epidemic that occurred during the 1960s. Congress gave the FAA's Administrator the power to regulate aircraft noise standards in 1968. The Airport and Airway Development Act made the FAA responsible for safety certification of airports served by air carriers in 1970. Following the terrorist attacks of September 11, 2001, Congress created the Transportation Security Administration (TSA), which succeeded the FAA as the agency with primary responsibility for civil aviation security.

During *Y2K*, not all of the FAA's activities were regulatory in the sense of coercive rules and policing activities. Under normal circumstances, in the course of performing its mission, the FAA worked with all airline organizations, both military and civilian, to provide research and support for common issues. However, in the case of *Y2K*, the FAA was scrambling as much as the other organizations in the air transportation sector to get its computer-based systems certified to operate after year 2000.

> [T]he FAA alone had more than 600 systems — and millions of lines of code — that had to be reprogrammed before the clock struck midnight. The U.S. had the added responsibility of leading the rest of the world's aviation systems through what had to be a seamless transition. And we did it. … Since 1997, we've completed more than 7,100 projects, installing new facilities, systems, and equipment across the U.S. and integrating them into the National Airspace System. We've done more than 10,000 upgrades of ATC hardware and software. Today, you can visit every one of our centers in America and won't find a single piece of hardware that's been around longer than I've been in this job (Garvey, 2002).

In October 1998, Delta initiated planning for a 'Home Stretch' meeting with the FAA to be held in January 1999, making sure that Mac Armstrong (Exec VP-Operations) would attend (Delta archive, ACT_ITMS.xls, 1999).

Hartsfield Atlanta International Airport

> At Hartsfield International Airport, one of the world's busiest, billing records are kept by hand (http://ajc.com, 1997).

Delta had such a strong interest in the Hartsfield Atlanta airport, that when the need for help to make the airport ready for *Y2K* was revealed, Delta offered to send its experts on loan. Delta sent Morgan of the *Airport Customer Service* business area (and former director of the code remediation project in Kiev), and Gravitt, a long-time member of the Delta family who had been running the PMO.

Industry

ATA / IATA / ICAO / ACI-NA

> Obtaining international information on airports and air traffic services has been difficult but is being made albeit slowly. All avenues for gaining information are being pursued (IATA, ICAO, ATA, FAA, White House *Y2K* Council, and Delta business units). ACS Regional Directors and Int'l Business Unit Leaders are assisting (Delta archive, EC Update0399.ppt).

The ATA served as the moderator and clearinghouse for *Y2K* activity, which at times included other critical groups such as Boeing and the FAA. (See the status report on air transportation organizations in Appendix E.) In December 1997, ATA member airlines met to begin formulating an approach for solving *Y2K* problems that were common to all members of the air transportation industry. Prior to this meeting, Price-Waterhouse had been assisting the ATA, and the working group recommended that they be retained as partners in the effort. In Price-Waterhouse's initial estimate, the airlines were expected to "reduce their total cost up to 75% by working together to solve common problems" (Delta archive, BODDec97.doc).

By January 1999, Delta encouraged ICAO to obtain the same level of critical system information from international airports that the FAA was obtaining domestically. Delta also requested status information on SITA and CUTE systems, and mail and bag sort systems. AIRINC (radio communications) was contacted with respect to testing opportunities. Delta Internal Audit division was engaged to audit ATA's databases (Delta archive, ACT_ITMS.xls, 1999).

As of May, reports indicated the following status of various organizations (Delta archive, "Delta Year 2000 Program Briefing Book," 1999, p. 14):

> FAA - still on target to be 100% completion by 6/99; recently reported that of 636 critical and non mission critical systems 90% were compliant with 89% of the mission critical systems ready; successful testing at DEN airport, additional testing being conducted in host computer systems and air traffic en route centers; Delta and other airlines are participating in FAA Contingency Planning workshops; working on a public communications plan; FAA inspectors making site visits to airlines (met with Delta 5/13/99); Jane Garvey and Ray Long have purchased tickets for 12/31/99 on AA; FAA's international focus is on areas that affect 60% of the domestic originated travel: Canada, Mexico, Bahamas, Japan, United Kingdom, [and] Dominican Republic.
>
> National Weather Service - Testing complete with positive results; awaiting documentation.
>
> NAV CANADA - Reporting *Y2K* Ready.
>
> U.S. Customs – U.S. Customs is stating computer systems will process data correctly but due to security concerns will not release documentation; individual customs offices do have contingency plans.
>
> ATA - On target.
>
> Airlines Clearing House (ACH) - Internal databases compliant, awaiting documentation from Chase Manhattan.
>
> Air Cargo Inc. (ACI) - State 2 systems are *Y2K* affected and both have been tested.
>
> Airline Industrial Relations Conference (AIRCON) - Compliant; completing disaster recovery plans.
>
> Airline Tariff Publishing Company ATPCO) – Compliant.
>
> Airline Reporting Corporation (ARC) - Internal systems now being addressed.
>
> SITA (Atlanta & London) - on target for 6/30/99 completion.

Summary

This chapter presented the context for *Y2K solution* that was provided by the Delta Year 2000 Program, and by external sector-based organizations. This context was common to all four business areas. The Year 2000 Program was highly structured, and provided a template for each business area to perform the same steps. All four business areas therefore had

- A common goal
- Common activities and reporting structures
- Common deliverables

These contexts have set the stage for understanding the factors in business area environments that led to their different solutions.

CHAPTER 7

PROGRAM ROLLOUT TO DELTA'S SUB-UNIT BUSINESS AREAS

> Environmental stimuli must be cognitively processed by actors—interpreted by individuals employing socially constructed symbol systems—before they can respond by taking action (Scott, 1995, p. xiii).

In 1998, Delta began a multiyear, billion-dollar-plus overhaul of its dated IT systems, which included implementing a new infrastructure design. At a time when other airlines were postponing expensive IT projects, Delta continued to invest beyond year 2000; $200 million was spent on new development during 2002, and this amount was to be a continuing item in the annual budget.

This chapter traces the history of the overhaul from within each of four sub-unit business areas. The changes were developed within the structure of the Year 2000 Program over the period from 1997 to 2003. The inclusion of the period beyond the year 2000 for this study, i.e., from 2000 to 2003, was essential in order to consider the results of the total IT transformation process. Because of timing and Delta's financial priorities, some elements of the *Y2K solution* that were chosen prior to January 2000 were not implemented until afterwards. Delta's financial condition, which became increasingly uncertain over the study period, affected IT expenditures. The World Trade Center attacks in 2001 affected the U.S. economy overall; and, the air transportation industry was especially wounded. The decline in numbers of airline passengers had a major impact and resulted in reduced revenues not only for Delta but also for all commercial air transport enterprises. Further, the cost of additional security scrutiny of passengers and the increasing cost of fuel produced increasingly enlarged expenditures.

Each of the four sub-cases presented in this chapter represents a setting for the parallel structured activities of the Year 2000 Program, which were not only embedded within the Delta organization, but also extended across to the external environment in each sub-unit system. Since Delta's main business was to provide air transportation service, the *Operations* area was naturally the largest and most influential of the core business areas. However, the other three areas *Airport Customer Service*, *Business Support*, and *Revenue*, provided essential supporting functions for *Operations*. Each of the four business areas had the same Year 2000 team structures, and the same process formats for carrying out the same Year 2000 Program activities. However, differences in other business area conditions led to different *Y2K solutions*. The aim of this chapter is twofold: to locate factors in the context of each of the business areas that led to its *Y2K solution* and then to assess each solution relative to contrasting organization performance models in light of the contextual factors.

Each sub-case presents one of the four core business areas in four sections.

- *Y2K solution*
- Functional and resource overview
- Institutional context
- Response assessment

The first section, *Y2K solution*, describes the actions of the business area in response to the *Y2K* problem. These actions are presented first in each case, since the existence of different solutions among the four business areas provided the structure for the research design, and served as the basis for the comparative investigation.

The second section, *Functional and resource overview,* presents a description of the task environment—size, locations, various other indicators of organizational complexity, and resources. Resources include key personnel and IT systems. Key personnel in each business area are named; names of any other relevant personnel are omitted, but their associated roles may be mentioned if necessary to explain an action more clearly. Because of the somewhat dynamic nature of the Year 2000 Program, a few of the leaders and team members changed roles and/or worked in different business areas or process areas of the Program at different times. Depictions of IT systems in each business area provide background and a baseline for the *Y2K* changes. Depictions include numbers of systems and desktop units, and condition of the systems in the form of summary metrics that were gathered as a part of the Year 2000 Program. Technical details of the assessment process are simplified, but are adequate for revealing conditions that existed at the time of the *Y2K* event.

The third section, *Institutional context,* presents the cultural character of the business area, which may include the presence of unions, ex-military employees, and / or other special circumstances; and the external regulative environment, which includes any external interconnections (industry and/or government) that were present.

Following the description of these background conditions in each sub-case, the fourth section, *Response assessment*, discusses the nature of the compliance response. The section presents conditions existing in the context of a business area that likely influenced its *Y2K solution*, and assesses the response as rational or institutional. Assessing a *Y2K solution* as rational or institutional characterizes the response with respect to the rival hypotheses, which are contrasting expectations for the influence of

context on actions. Rational responses correspond to a rational-contingency model. Institutional responses correspond to an institutional model.

A solution assessed as rational is a solution that is

- the result of a rational choice process based on adequate information and,
- the optimal choice for managing complexity, therefore decreasing uncertainty / increasing predictability, and / or increasing efficiency.

Evidence of adequate information includes that a business area sought a variety of information sources, e.g., consultants and vendors with high reputations and understanding of best practices, along with high quality internal sources. Evidence of a rational process in the business area is increased predictability or increased efficiency (increased revenue, reduced cost, or other measure), cost management or staying in budget.

A solution assessed as institutional is a solution that is

- not the result of a rational choice process (because of complexity or time constraint or both), therefore the choice is based on
  - inadequate information (either limited or low quality) and / or
  - sectoral influences (cultural, competitive, or regulative conditions) and / or
  - copying the solution of others (models of experience)

Evidence of the possibility for inadequate information and an institutional choice process is complexity and / or time constraint. Evidence of an institutional solution is decreased predictability or decreased efficiency (reduced revenue, increased cost, or other measure) in the business area, a solution required by regulations or other regulative circumstances

such as enhancing the image of the airline, or a solution representing a technology or COTS product that is a popular choice, but not necessarily a fit with the activity.

The environmental factors relating the theoretical analysis of the *Y2K solution* in the sub-case are presented in tabular form, along with a brief discussion, at the end of each sub-case section. An elaborated discussion of factors is presented in Chapter 8.

Sub-case 1: *Airport Customer Service*

> … at Delta's gates, there are few, if any, queues in front of the agents' desks … Instead, many passengers stand, trancelike, before big-screen, flat plasma displays. The monitors flash every few seconds. All this information comes into the displays via the Delta Nervous System, which pulls information from Delta's various databases and pushes it onto the gate displays (Gage and McCormick, 2003).
>
> [T]he Airport Renewal project is the #1 project at Delta Technology, and a large part of the organization is focused on rolling out the new infrastructure worldwide over the next 18 months. Roughly 250 people are allocated to the project, working in teams on support, deployment, development, procurement, and equipment. Phase One—renewal of Delta's top 20 airports and deployment of the CustomerCare application—is scheduled for completion by the end of this calendar year when Delta will have rolled out about 20,000 pieces of hardware (Harding, 1999).

Y2K solution

In response to the mandate for *Y2K* compliance, the *Airport Customer Service* business area replaced the majority of their systems. The Year 2000 Program team in *Airport Customer Service*, in conjunction with the Airport Renewal project, designed and installed a completely new infrastructure for airports, where high bandwidth data networks connected to the DNS and new standardized desktop units replaced a hodgepodge of PCs and green screens.

The Human Factors team at *Delta Technology* designed the integrated software system, called the "CustomerCare" system, which included the design of information on displays that accounted for various aspects of usability.[106] A number of other specialists assisted in the development, from technical systems experts to gate agents. Fourteen gate agents contributed to the gate design, which included various programs for providing and presenting information to customers, and, to ticket and gate agents, and other *Airport Customer Service* employees. Informal polling of customers in the gate areas contributed

[106] The Human Factors team comprised a group of specialists who were educated at Georgia Institute of Technology; most had degrees from the graduate programs in HCI and Digital Media.

to understanding what information elements and delivery media worked best—even to testing whether a male or female voice was better for communicating messages in the gate area. A prototype of the system was installed in the Jacksonville, Florida airport in September 1998. The Jacksonville station manager was so enthusiastic that he wanted to install it immediately in the other four Delta gates. However, according to Feld,

> as a prototype, it was held together by "bailing wire." The system could not be reproduced without further modifications. The manager therefore stopped the flights and sent them all through the one demo gate!

Airport rollout was 14 months from prototype to installation. Rollout continued to Atlanta, Salt Lake City and Cincinnati beginning in 1999 and to other airports after year 2000.

For customers entering the airport, kiosks were installed to allow passengers more efficient check-in and to reduce wait times. Customers could use these kiosks to access boarding passes, itineraries, and receipts. Large display screens were placed at each gate for departing customers. Program output displayed up-to-date information about flight schedules, seat assignments, upgrades, boarding times and boarding order, crown room and restroom locations, etc. For customers deplaning in hub airports, the screens also displayed the location of connecting flights. Apart from the improved customer service, and efficiency of operation, the CustomerCare system significantly enhanced the integrity, reliability, availability, and accessibility of the information that existed in the *Airport Customer Service* area prior to *Y2K*. The system received the Computerworld Smithsonian Award for Technology Innovation in year 2000.

In addition to replacing hardware and introducing the DNS-powered software in airports, similar systems were installed at Delta's 12 major call centers. Table 17 shows

the new systems developed for *Airport Customer Service* that had replaced airport systems that were at risk.

Table 17: *Y2K solution* in *Airport Customer Service*

AIRPORT CUSTOMER SERVICE		
Function	**System**	**Vendor**
Fiberoptic networks installed at airports and call centers		
Standardized PC systems replaced older PCs and green screens		HP
Large screen display	Gate Information Display System (GIDS)	*Delta Technology*
Flight-information	Flight Info Display System (FIDS)	*Delta Technology*
Gate agent / boarding passengers	Cornerstone	*Delta Technology*
Baggage handling		
Kiosks	TouchPort	Kinetics

The condition of systems and the Future Vision goals for *Airport Customer Service* strongly influenced the design of its *Y2K solution.* The influence of its wider institutional environment was evident in the familiarity of the environment for the new technology, the presence and availability of networking products and technical expertise in the marketplace, and only minimally from government regulations. Government influence was through their activities in funding research that influenced solutions.

Functional and resource overview

The *Airport Customer Service* business area comprised the divisions of Delta that performed customer-facing functions. *Airport Customer Service* was concerned with customer activities from the time of entering the airport to boarding the plane. These functions were predictable, repetitive customer interactions—essentially tracking the customer and his/her baggage through airport facilities. Names of the *Airport Customer Service* divisions, which included 58 different personnel department numbers (PDNs),

revealed the nature and variety of activities in the business area and provided evidence of the complexity of the business area. The division names were also an indicator of specialized roles and occupations. Of the four core business areas, the activities of the *Airport Customer Service* divisions were among the most visible to the public, but among the least complex. However, the approximately 180 different locations for many of these activities, as shown in Table 18, added a dimension of complexity.[107]

Table 18: No. of divisions and no. of locations in *Airport Customer Service*

DIVISION	NO. OF PDNs	NO. OF LOCATIONS
Airport Customer Service (ACS)	33	180 airports plus Atlanta campus
Cargo	n/a	
Consumer Marketing	5	1
CustomerCare	2	1
Delta Shuttle	5	n/a
Distribution Planning	1	1
Reservations (RES)	12	15
TOTAL	58	180 airports plus Atlanta campus

Table 19 shows the various functions that the division performed.

Table 19: Functional activities in *Airport Customer Service*

Customer service & operations
Finance, business solutions
Domestic & int'l line operations
Domestic station mgmt, Ops & services
Training, personnel dev & communications
Assistance center
Business partners
Ramp tower
Airport courtesy driver
Domestic gates / FTO
Crown Room club & G.O.
Domestic fuel operations & cabin service

[107] The columns headed by the titles "NO. OF PDNs" (personnel department numbers) and, "NO. OF LOCATIONS," show the total number of divisions and geographic locations included within the business area. Some of the individual division metrics could not be obtained.

Table 19 continued

Domestic skycap service
Int'l lounges in domestic locations
International station mgmt
Int'l field operations (ramp)
Int'l gates, security, cabin & skycap
Reservations sales
Res sales admin & training
CTO, domestic & int'l
Distribution planning
Relationship marketing
Marketing communications
Product planning
CustomerCare
Baggage service
Shuttle & management

In *Delta Technology*, the Customer Portfolio division managed all of the IT systems that supported the *Airport Customer Service* business area of Delta. In 1997, 119 systems were their responsibility. Hartsfield airport in Atlanta, the location of the most activity for Delta, had 149 systems, mostly proprietary to the airport. The only interface with *Delta Technology* was the baggage sort system. Landing lights, elevators, escalators, landing security system, etc. were owned and maintained by the City of Atlanta.[108]

The Customer Portfolio consisted of 5 sub-groups, including, Airport Customer Service (ACS), Reservations, Distribution Planning, Consumer Marketing, and CustomerCare (formerly called Consumer affairs, and included baggage service). The divisions shown in Table 18 reflected these groupings.

The personnel shown in Table 20 served as leaders and decision-makers for the replacements and upgrades that were performed for the Year 2000 Program in this area.[109]

---

[108] Note: the software for the landing light system was written by two Georgia Tech graduates—brothers who did the work as independent contractors.

[109] A date beside a name in this table refers to the date of the Delta report that shows the assignment.

Table 20: Year 2000 Program team in *Airport Customer Service*

DELTA	*DELTA TECHNOLOGY*
Delta Exec Sponsor: V. Escarra, Exec VP – *Airport Customer Service*	
Delta Portfolio Owner: V. Escarra	*Delta Technology* VP: Keith Halbert
Delta Portfolio Manager: June Fox (5/'98)	*Delta Technology* Portfolio Manager: Chuck Creech
Delta Portfolio Director: Robin Stricklin	
IT systems not maintained by Delta Technology[110]	*IT systems maintained by Delta Technology*
Worldspan	*Y2K* Team Leader: Neal Morgan (9/'97)
	Y2K PD: John Jacobi
	Customer Portfolio Lead: Kevin Hutcheson
	Customer Team Coordinator: Richard Hardy (12/'97)

Vicki Escarra, Executive Vice-President – *Airport Customer Service*, played an active and key role in the successful planning and implementation in this area. Escarra was a long-time member of the Delta "family." Describing her enthusiastic involvement with the airport renovation, Feld said, "Vicki Escarra was phenomenal at rallying the troops" (Feld, 2006). On the *Delta Technology* side, however, Keith Halbert and Neal Morgan were outsiders. Halbert was a contractor who worked at Delta as a member of The Feld Group, the consulting group led by Feld. Morgan was hired at Delta in 1996 following a successful career in the U.S. military. Both Halbert and Morgan had extensive experience with networked IT systems. The following individuals participated in the identification, analysis, and solution development effort for the Customer Portfolio of Airport Customer Service (ACS).[111]

[110] Note: The category "IT systems not maintained by Delta Technology" included systems in external facilities and operated by external vendors. (Delta archive, Metrics.xls).

[111] In this table, DT refers to a *Delta Technology* employee; DL refers to Delta.

Table 21: Employees on the Customer Portfolio (ACS) team

NAME	ROLE
Liz Boothe	DL - Reservations Desktop Coordinator
Cheri Burbage	DT - Desktop Support Analyst
Don Burgoyne	DT - Reservations Field Services Support
Clyde Eaton	DL - Customer Portfolio SME
Mark Griffin	DT - Field Services Support
Jerry Hall	DT - ACS TPC
Glenn Harper	DT - Customer Care SME
Melanee Haywood	DT - Desktop Lead Analyst
Bill Jeffrey	DT - Field Services Support
Timothy Johnson	DL - Distribution Planning Coordinator
Jeani Jones	DT - Call Center Renewal
Fred Juch	DT - Airport Renewal Deployment
Sherri Kadel	DT - Call Center Renewal
Bryan Lamberth	DT - Airport Renewal Liaison
Rhonda Morris	DT - Call Center Renewal
Lisa Peters	DT - Workgroup Engineering
Dale Piper	DT - Airport Renewal Liaison
Paul Redemske	DL - ACS Desktop Coordinator
Pat Roberts	DL - Consumer Marketing Coordinator
Cathy Spencer	DT - Customer Care Field Services Support
Chuck Tatum	DL - ACS SME
Randy Tiemann	DL - Customer Care Coordinator
Ken Ward	DT - Workgroup Engineering

The Customer Portfolio team took the following actions in phases according to the process design template: (1) inventory and assessment, (2) migration planning, (3) code remediation, and (4) desktop renewal. This process in *Airport Customer Service* was identical to that of the other business areas. However, the focus on system replacement and improving the customer experience ultimately overrode the focus on *Y2K*.

The team's first action was to inventory the systems to learn what they owned, and to assess this body of systems for planning purposes. The number of systems, their complexity, and other attributes were assessed during this initial phase. This was a very difficult stage of the process. Many of these systems and their hardware devices were among the oldest and most outdated of the Delta systems. The nature of the systems—the

fact that they were old and that no one had known before how they all interacted in total to produce their collective outputs—contributed to the difficulty. Results of the first phase, the inventory and assessment actions, are shown in Table 22 and Table 23, which indicates the level of complexity that existed in the systems in this division. The inventory identified the systems; the assessment phase classified them based on their criticality to the functioning of the business area. They were listed as high, medium, and low to reflect these assessments.[112]

Table 22: Assessment metrics for systems in *Airport Customer Service*

NO. OF SYSTEMS			NO. OF LANGUAGES	LOC (millions)	NO. WAIVERED SYSTEMS	NO. DESKTOP UNITS
HIGH	MED	LOW				
36	35	48	13	6	9	See footnote.[113]

Table 23: Programming languages and date fields in *Airport Customer Service*

LANGUAGE	LOC	DATE FIELDS	DATE FIELDS AFFECTED	PERCENTAGE OF OCCURRENCE
Assembler	3,600			0.00%
C	225,498			0.00%
C++	766,756			0.00%
COBOL	18,517	634	232	1.25%
Delphi	133,341			0.00%
HTML	90,933			0.00%
Natural	203,831	29,813		14.63%
Oracle	1,500			0.00%
ProC	16,514			0.00%
SQL	1,877	317		16.89%
ScriptWrite	224,744			0.00%
VBA	108,180			0.00%
Visual Basic	30,431			0.00%

[112] The classification (HIGH, MED, or LOW) indicates the critical nature of the system to the functioning of *Airport Customer Service.* The classification was assigned during the assessment phase based on a variety of scan information.

[113] "There were over 6000 desktops in the Atlanta airport alone" (Feld, 2006). An accurate number for the total was not available.

Migration planning was the phase where the team confirmed action plans. In the code remediation phase, the code that had been previously identified as containing the *Y2K* bug was sent to one of two outside organizations to be cleaned. In the desktop renewal phase, desktop units were replaced with standard models identified by division. The other data shown in Table 22 are the number of programming languages represented, the lines of code (LOC) requiring remediation to eliminate the *Y2K* vulnerability, the number of waivered systems, and the number of desktop units assigned to the area.[114]

In the *Airport Customer Service* area, there were 53 current state computing models (existing hardware and software configurations). Attempting to conform these models to the Future Vision standards, the number was reduced to 23 solution models (Delta archive, 1999, Customer Summary Document.doc).

Table 24: Desktop models in *Airport Customer Service*

DIVISION	CURRENT STATE MODELS	TRANSLATED TO SOLUTION MODELS
ACS	28	10
RES	18	10
Distribution Planning	1	1
Consumer Marketing	5	1
CustomerCare	1	1
TOTAL	53	23

Institutional context

Cultural character

The concern for customer satisfaction at Delta was strongly related to the notion of southern hospitality. In Delta's tradition, this approach was directly an outgrowth of how "company" would be treated when visiting in your home. In fact, most Delta

[114] Language and waivered system metrics from (Delta archive, "Assessment Summary Report of Dec 31, 1997," 1997).

veterans viewed the changes in the airport as an extension of this attitude and level of consideration. Employees had used technology in this business area from "way back." However, the problem with the earlier *Airport Customer Service* systems was the cryptic interfaces, reminiscent of early PC experiences, and the incomplete and outdated, therefore inaccurate information that was provided. In many cases, the boxes that the Delta gate agents were so adept at using were only "green screens," i.e., terminal systems, and had no processing capability at all. The systems were limited in assisting the agents.

Regulative environment

Government agencies

The institutional environment of *Airport Customer Service* had fewer regulative aspects than the other business areas. The regulative structure most "present" was the airport authority. In the U.S., airports are operated by various government entities, usually a county or city authority.

The structural protection that the government provided for Delta personnel and various contractors (legal contracts, pension protection) was no different in *Airport Customer Service* from that of other Delta business area environments. However, systems design and use of Delta's reservations systems and its security screening did reflect its particular regulatory requirements. Reservation systems were the concern of the DOT. The Sabre system of American Airlines was the first computer reservations system (CRS). The first "yield management" program used information from Sabre to understand customer buying patterns to help determine the optimum pricing for seats and the first cheap but nonrefundable fares. Observing the competitive advantage that

American had with the CRS, the DOT imposed regulations that governed the use of such technology (Gage & McCormick, 2003). Delta's reservations systems had been operated by Worldspan since 1990, where Delta was both a Worldspan owner and a customer. For the Year 2000 Program, Delta appointed a liaison for communicating between Delta and Worldspan regarding its *Y2K* status. The Worldspan systems were declared *Y2K* compliant by mid-1998.

Rules for security screening affected the design decisions of airport systems and the security process in the airport facilities. One informant, who worked on the *Airport Customer Service* Human Factors team said,

> Delta improvements can only progress to a point. Delta is controlled by airport environments, the control tower, and other constraints. For example, TSA ruled that a customer must have a printed boarding pass to go to the gate area. DT worked with IBM and other vendors to address such concerns.

The security screening process was historically the duty of Delta's ticketing and gate agents. However, TSA requirements would change Delta agent responsibilities dramatically after 9/11. As Mullin said,

> Delta now has a "new partner" [the U.S. government] in that passengers are not totally under Delta's control between the airport and the plane.

One Delta informant described his encounter with a new Homeland Security Department TSA security agent when the screening processes were being changed.

> … communication with the TSA deputy resulted in impasse. The guy has a state police background … speaks a different language.

Industry relationships

Various relationships existed in the *Airport Customer Service* environment that required special processing to eliminate *Y2K* concerns. The Airport Customer Service (ACS) division contracted directly with suppliers for labor, and these contracts were processed and stored as electronic files. ACS issued labor contracts (Ground Handling

Agreements) for under wing services that include ramp, cabin cleaning, security screeners, skycaps, janitorial, transportation on airport grounds, waste removal, etc. Ticketing (code-sharing) agreements existed for entities using certain specialized computer systems, particularly Scandinavian Airlines (SAS) and South African Airlines (SAA) computer systems. The Cargo division had approximately 25 agreements with General Sales Agents (GSAs) to sell cargo space on Delta's behalf from an international perspective. Informants believed that those GSAs were independent of any other business area's GSAs. The *Airport Customer Service* business area was also responsible for conducting the inventory, assessment, and treatment phases related to facilities' leases entered into by Cargo (Delta archive, Defnote1.doc).

Table 25: Year 2000 Program snapshots – *Airport Customer Service*

DATE (MM/YY)	Y2K ACTIVITY
1998	Remediation of the Deltamatic reservation system, hosted by Worldspan, is complete
Sep 1998	Jacksonville prototype. New system installed "live" for user testing
2000	CustomerCare systems installed in hub airports
2002	Reservations call centers established and operational.
2003	Airports with DNS connection totaled 81.

Response assessment

> We started down this path prior to *Y2K*. As we looked at the technology that was in our airports we felt that there was lower risk to actually going in and replacing the technology that was there than trying to remediate it for *Y2K* (Robb, quoted in Murray, 2002, p.1).

The condition of the *Airport Customer Service* IT systems drove the decision to "plow the field and replace," which was assessed as rational, even though institutional aspects of the decision and its development constraints were apparent. This business area was a top priority for the new CEO at the outset because of Delta's recent history of poor customer service, undoubtedly a result of prior financial problems and associated

cutbacks. The leaders charged with the mission to improve customer service via IT systems were deep in experience and understanding of how to make it happen. The IT staff was similarly well equipped—the "best and brightest." Further, the decision was consistent with Future Vision concepts. The "Future Vision" refers to a new generation of technology capabilities that will enable management of the overcrowded national airspace system (NAS) into the future, a vision conceived by researchers under various government contracts (e.g., NASA, RTCA).[115] The decision was also consistent with the experience of CIO Feld and his consultant group.

It is notable that the evolutionary thinking regarding the ATC systems is related to the overcrowding of the air space. The models of air transportation management have changed very little in concept since the early days of passenger flight. The imprinting of this model has held even as the numbers of passengers and aircraft have been increasing, and while other aspects of the air transportation environment have been changing. The air traffic controllers are overworked and many airports are understaffed. The job is stressful and taxing on the processing power of the human brain. However, it is "the way these things are done" (Scott, p. 505). Since there is a saturation point in air traffic, given the capacity of the airports and the capabilities of the aircraft, the Future Vision concepts have been part of an initiative to develop technologies that are different from those that are no longer working to solve the problems, and that have implications for safety. It is also notable that Delta was influenced to pursue the Future Vision changes by regulatory sources, and by consultants.

[115] These conceptions have included a number of features related to the use of IT to extend the capabilities of air traffic controllers.

The decision to replace equipment and to modernize resulted in increased predictability, especially considering the age of the systems and the possibility that unknown "features" in the code carried negative consequences for their operations. However, the decision process did not include consideration for all of the possible consequences of how the current hardware and software might coexist within the DNS architecture without changes. Nor did the decision process include consideration for the multitude of ways where costs could have been eliminated by keeping pieces of the existing systems. However, if such a detailed analysis were feasible, the time and cost of the process would likely have outweighed the cost of the solution they chose given the 36,000 desktop units and thousands of interconnecting pieces of networking equipment and systems.

Delta adapted the overhaul to fit their financial condition by putting off projects that would take more than a year to pay off (like new baggage-handling systems) and accelerating others that would cut costs immediately and possibly increase revenue (like increasing the number of self-service kiosks and replacing call center systems). Systems were rolled out gradually, to just one or two hub airports instead of to all 40 domestic airports, with the intent that once the financial situation turned around they would be ready to speed up implementations. Since Delta was among several carriers that had continued to receive low marks in prior years for many functions in customer service, lost baggage being one, it was an obvious way to improve customer relationships and improve turnaround efficiency in the process.

Turnaround at the gate was important to the overall flight operation in a number of ways. Delays at the gate for any reason created problems, but most important to Delta

was their effect on the bottom line. One airline analyst estimated the cost of delaying a departure could run as high as $500 a minute (Gage and McCormick, 2003). In an interview with Delta's Finance division reported in 1997

> that irregular operations cost Delta about $20 million per month to cover hotels and meals for interrupted passengers, tickets on other airlines, baggage delivery extra crew costs, ACS overtime, and monetary compensation to inconvenienced passengers ("On-time fix requires cross-divisional commitment," 1997, p. 11).

Prior to *Y2K* and the Airport Renewal project, gate agents had a limited view of what was going on that affected the efficient boarding of the aircraft, and that ultimately affected the satisfaction of a customer. The *Y2K solution* changed that. The real-time information that was provided by the new systems enabled all Delta personnel to have the same view of all activities. Further, customers could interact with the systems themselves—via delta.com and other system interfaces—to make reservations, purchase tickets, and check in for flights. Customers could access the DNS through any data device, such as computers, PDA's, pagers, cell phones, and gate displays and readers; therefore, the numbers of Delta personnel required to assist customers was dramatically reduced, and that reduction contributed to major ongoing cost reductions. The interaction capabilities using the interface devices also enhanced Delta's image as a high tech player. These benefits extended to baggage handlers and ground equipment personnel, and to travel agents via CRS systems—other ways in which the integrated systems improved business area performance. This is an example where the state of the technology—within the institutional environment—drove solution possibilities. Even if money had been no object ten years earlier when the *Y2K* bug could have been eliminated, the possibility for solutions would have been different conceptions, and development and implementation

would have taken much longer. The rationality of the decision within this scenario, however, would likely have been similar.

The rationality as evidenced by the financial benefit is clear. The following is the estimated cost reduction that resulted from replacing and modernizing the *Airport Customer Service* systems:[116]

Personnel reduction:

- Gate agents: Delta's main airports have an average of 50 gates. The new systems in 81 airports reduced personnel from 3 to 5 agents per gate to one agent per gate, saving from $324 million to $486 million a year (based on $40K annual salary).
- Ticket counter agents: Delta's main airports had required 50 people for two shifts prior to installing kiosks. Using a kiosk, a single ticket agent could check in three people at once, which reduced personnel from 3 counter agents to 1. With 81 airports using the system, Delta could experience a total savings of between $107 million and $110 million a year (based on the total salaries for these positions—between $640,000 and $680,000 per airport).

Improvement in baggage handling:

- Delta's cost for a lost bag was around $150 to locate it and return it to its owner. In 2002, for every one thousand customers Delta baggage handlers lost 3.57 bags. In 2001 the lost bag count was 4.11 bags per thousand. The improvement saved Delta $8.7 million.

This cost reduction improved Delta's financial condition and improved the customers' experience, which could bring additional revenue in increased numbers of repeat customers.

Sub-case 1 summary

The *Airport Customer Service* business area of Delta served as Sub-case 1. The sub-case description included its *Y2K* compliance response (*Y2K solution*) and the context for this action provided both by the conditions in the *Airport Customer Service*

[116] See Gage & McCormick (2003).

business area and by its sectoral environment. The functions of *Airport Customer Service* were routine. The customer interaction was dynamic. The *Y2K solution* included remediation of code in existing high critical systems in order to remove the *Y2K* vulnerability and replacement of systems across the board where possible. The context included airport restrictions, and various legal arrangements with contractors and employees, but otherwise a neutral area from a regulative standpoint with a couple of exceptions: reservations systems and security screening. The DOT and the DHS / TSA regulated and monitored those activities, respectively. However, the regulations did not affect *Y2K solution* decisions appreciably. Table 26, Table 27, and Table 28 summarize the information from this sub-case.

Table 26: *Y2K solution* in *Airport Customer Service*

AIRPORT CUSTOMER SERVICE		
Function	**System**	**Vendor**
Fiberoptic networks installed at airports and call centers		
Standardized PC systems replaced older PCs and green screens		HP
Large screen display	Gate Information Display System (GIDS)	*Delta Technology*
Flight-information	Flight Info Display System (FIDS)	*Delta Technology*
Gate agent / boarding passengers	Cornerstone	*Delta Technology*
Baggage handling		
Kiosks	TouchPort	Kinetics

Table 27: Summary metrics in *Airport Customer Service*

TOTAL NO. OF DIVISIONS	47	
NATURE OF WORK	Routine / dynamic	
LOCATIONS	180 airports plus Atlanta	
TECHNOLOGY PROFILES	1997	2003
Application systems	119	129
# High/Med/Low critical systems	36/35/48	36/34/59
# Languages	13	
# LOC (millions)	6	
# *Delta Technology* systems	119	

Table 27 continued

# Waivered systems	9	
# Desktop units		20,000 [117]
# Desktop models, original	53	n/a
# Desktop models, solution	23	n/a
Intro computer processing date	Deltamatic reservations system 1964	
DOMINANT INDUSTRIES (fields represented)		
	Customer relations	
ENVIRONMENT		
GOVERNMENT	Airport authority, DOT, TSA, Customs, INS etc.	
CULTURAL	Non-union	
INDUSTRY	Employee contractors	

Table 28: Summary of environmental factors in *Airport Customer Service*

FACTORS	INSTANCE
Public image	Airport displays and kiosks
Belief systems	Family, "southern hospitality"
Existing practices and routines	New airport environments were simply reformulations of the familiar, propagating the imprinting of institutional arrangements.
Industry relationships	Ticket processing, travel agents
Regulations	Airport rules, security, privacy, competition
Mimesis	"Airport of the Future," elements of BNI solution
Goals	Improve customer service while removing *Y2K* bug
Cost management	Deferring rollout to new airports depending on budget

Given the *Y2K solution* in *Airport Customer Service*, its context was examined in order to assess the rationality or institutionality of the decision as an alternative for solving the *Y2K* problem. The solution was assessed as rational, even though a number of institutional influences were noted. Table 29 shows the factors related to the assessment.

[117] This number is an estimate based on extrapolation of the ~6,000 units at the Atlanta airport.

Table 29: Factors related to the *response assessment* in *Airport Customer Service*

OPERATIONAL DEFINITIONS	FACTORS: RELATED TO *Y2K Solution* in *AIRPORT CUSTOMER SERVICE*
Institutional model	(*Y2K* Contingency: *Y2K bug*)
CATEGORIES OF EVIDENCE RELATING TO AN INSTITUTIONAL PROCESS	FACTORS THAT CONTRIBUTED TO AN INSTITUTIONAL PROCESS
<u>Cultural</u> • Related to a social fact: perceptions of air transportation, information technology, information security, safety & other values • Cognitive, e.g., Delta family culture • Familiarity with service orientation, comfortable, habitual, routine • Related to established relationships, e.g., vendors • Inadequate information and experience with changes to systems in the Internet environment • Inadequate information and experience by both Delta and by consultants as to responsibility for security	1. <u>Conditions in the business area and its IT systems:</u> • Systems working but without documentation • Systems woefully out of date • IT employees content with the status quo • Habit of avoiding outside consultants 2. <u>Character of the business area environment:</u> • Inadequate conditions in government agency charged with oversight (DHS / TSA) 3. <u>Distraction of other business area contingencies:</u> • Financial status • Economic conditions • Competing airlines
CATEGORIES OF EVIDENCE RELATING TO INSTITUTIONAL DECISION-MAKING	FACTORS RELATING TO INSTITUTIONAL DECISION-MAKING IN RESPONSE TO *Y2K*
<u>Regulatory</u> • Requirements for maintaining organizational legitimacy <u>Mimetic (Following the crowd)</u> • Research from institutional sources • Fashionable, popular • Recommended by vendors • Inadequate information about products and experiences outside organizational boundaries (reports only about successes)	4. <u>U.S. laws, industry regulations:</u> • Industry regulations were focused on protecting the competitiveness of air transportation, not information security • U.S. govt agencies' systems not *Y2K* compliant • Industry regulations focused on passenger screening after 9/11, but inadequately researched, equipped, and trained. • Industry regulations linked to intelligence gathering—a public concern strongly related to privacy, but not linked to information security 5. <u>Character of business area environment</u>: • External chaos because of time limitation • Mixed understanding of the risk • IT products available in the marketplace

Table 29 continued

Rational-contingency model	
CATEGORIES OF EVIDENCE RELATING TO A RATIONAL PROCESS	FACTORS THAT CONTRIBUTED TO A RATIONAL PROCESS IN IT MANAGEMENT
Goal orientation Actions relating to efficiency and effectiveness Communications related to mission control	1. Leadership: • Acted on the opportunity to improve operations, which made the enterprise more competitive • Applied human factors and field testing to assure usability • Stayed actively and personally involved in order to insure success. 2. Condition in the business area and its IT systems: • Process put in place to assure continual assessment with respect to condition of systems and efficiency of performance 3. Responses to business area contingencies: • Management of financial condition (e.g., delaying airport rollouts based on budget priorities)
CATEGORIES OF EVIDENCE RELATING TO RATIONAL DECISION-MAKING	FACTORS RELATING TO RATIONAL DECISION-MAKING IN RESPONSE TO *Y2K*
Regulatory Requirements for maintaining organizational effectiveness Decision-making criteria • Based on knowledge of systems o *Y2K* compliance o Fit with functional area o Efficiency related to cost, processing, resources, etc. o Security	4. U.S. laws, industry regulations: • Even though limited and late in coming, a bounding framework of concern by govt/industry rules wherein the condition of IT systems is recognized as vital to safety and national security. 5. Leadership: • Knowledgeable about the value of information accuracy and availability • Understood the contribution of IT to the functioning of the organization • Employed personnel with high levels of skills • Adequately responded to security contingencies 6. Character of the business area environment: • Personnel resources were adequately aligned with requirements • IT products to serve the needs in *Airport Customer Service* were available in the marketplace

As the above information indicates, there were both institutional and rational influences that weighed into the Airport Customer Service decision. The rationality of the decision is obvious with respect to the financial benefit of the decision. The institutional character of decisions is implicit in the actions. Evidence of the imprinting of airport operations was preserved for the most part by the design of the systems. A customer still

has the same basic look and feel of the airport experience, even though the technology changes have been dramatic. Gate and ticket agent numbers were reduced, but their function and their presence is the same from a customer perspective. Delta *Y2K* teams, both developers and installers, had to interact with the airport authorities in order to be compliant with the rules of their facilities, which for the most part are just as they have always been. However, the changes Delta made to various reservations systems affected the very existence of travel agents in the Delta environment, a case where the *Y2K solution* actually influenced its institutional context.

Travel agents as a body of workers has been systematically removed from interaction with Delta, beginning with the establishment of Worldspan, and then followed by the creation of the various modes by which customers can take action directly in arranging for their own travel. This institutional factor has been "virtually" eliminated and made non-essential as a design consideration for IT systems.

The state of the technology application in Airport Customer Service may be described as completely current with all of the latest technical capabilities in computer-based processing. This reflects the growth and evolution of the IT industry, and the changing nature of the air transportation industry with respect to in-house vs. proprietary programming code. In view of the fact that some of these same institutional influences and effects regarding technological changes have appeared in other sub-cases, these factors are discussed further in Chapter 8 as a part of the cross-case comparison.

Sub-case 2: *Operations*

> More than mechanical wizardry, it was computers that transformed transportation in the late 20th century. … Advanced computer systems in air traffic control tracked 32,000 flights per day (Smithsonian National Museum of American History. "Transportation Technology, 1950-2000").
>
> Airline Operations Portfolio … has the majority stake in Year 2000 (Delta archive, dt43, 1998).

Y2K solution

Besides code remediation and other aspects that were carried out in all of the business areas, the notable *Y2K solution* in the *Operations* area took place in the Technical Operations (Tech Ops) division. In an effort to support the activities in Tech Ops with greater efficiency, Delta made a commitment to lease a commercial off the shelf (COTS) product from SAP, which enabled complex enterprise resource planning (ERP) and the integration of multiple functions across the Delta enterprise.[118] Using this software, Delta decision makers believed that integration of activities in inventory management, supply chain, and the finance function could provide benefits.

Because of its complexity (and possibly the expense), the installation of SAP was deferred until after the rollover (Overby, 2003). Tech Ops would then use it to aid in managing $1 billion worth of aircraft parts inventory. A system called Xelus, which enabled planning for parts based on demand, was linked with the SAP system. To document aircraft repairs, the Creative Concepts company supplied software, which enabled technicians to access all manuals and other technical information online.

---

[118] SAP was a leading provider of enterprise resource planning (ERP) software, which was used to integrate functions such as human resources, accounting, manufacturing, and distribution. By 2007, SAP customers numbered over 27,000 companies worldwide (Hoover's, 2007).

Following a failure in the flight attendant scheduling systems after year 2000 rollover, Accenture was contracted to perform the analysis and integration for a new system. This project, like most systems work, was interrupted after 9/11, but continued after the crisis had abated. Table 30 shows the *Y2K solution* in *Operations*. The conditions in the *Operations* business area influenced these *Y2K solution* decisions in a number of ways.

Table 30: *Y2K solution* in *Operations*

OPERATIONS		
Function	**System**	**Vendor**
Flight assignment	Coldstart	Developed with Ilog
Flight-tracking	Total Dispatch	*Delta Technology*
Supply-chain	mySAP	SAP
Supply-chain mgmt	mySAP Business Suite	SAP
Parts management	Xelus Plan, Xelus Extend	Xelus
Technical documentation		Creative Concepts (Gen'l Dynamics subsidiary)
Crew scheduling		Jacada, Accenture

Functional and resource overview

Operations was the business area that performed the crew, flight, and aircraft maintenance functions—the central functions of airline service. Conceptually, the other three business areas performed support functions for *Operations*. *Operations* was the largest as well as the most complex of Delta's four business areas. Its 40,000+ employees represented over 60% of the Delta organization. As shown in Table 31, the 248 different PDNs and the location of operations at 180 different sites were evidence of the scope and complexity of *Operations*.[119] As another distinguishing aspect when compared to the other Delta business areas, *Operations* presented the most concern for regulators, such as

[119] The column headed by the title "NO. OF PDNs" (personnel department numbers) shows the number of sub-divisions included within a division named in this list; e.g., Flight Ops has 35 sub-divisions.

the FAA. For example, because the FAA was responsible for certifying the pilots and the condition of the aircraft, the agency had an obligation to monitor key activities in the *Operations* area. To handle the issues related to regulations of the FAA and others, *Operations* had established two divisions: FAA and, Corporate Safety and Compliance, which is evidence of the organization's adaptation to its institutional environment.

Table 31: No. of divisions and no. of locations in *Operations*

DIVISION	NO. OF PDNs	NO. OF LOCATIONS
FAA	1	1
Corporate Safety and Compliance	1	1
Operations Control Center (OCC)	1	1
In-Flight Service (IFS)	18	180 airports plus Atlanta campus
Flight Operations (Flight Ops)	35	180 airports plus Atlanta campus
Ops Management		1
Aircraft Crew & Resource Mgmt		
Airport Customer Service (ACS) – ACC & Back office		
Airport maintenance / Ground Support Equip (GSE)		
Ground Ops		
Flight Ops – campus		1
Shuttle	1	A number of U.S. airports
Technical Operations (Tech Ops)	191	nearly 50 U.S. and foreign locations
Maintenance & Inventory		
Engine Comp & Hanger Ops		
Technical Operations Center (TOC): shop, offices, bays & hangars		1
DFW hangars		1
TPA hangars		1
TOTAL	248	180 airports plus Atlanta campus

The Airline Operations (Air Ops) Portfolio division in *Delta Technology* was responsible for managing all of the IT systems that supported the *Operations* business area of Delta, which numbered over 200 systems. The individual Air Ops systems were combined into sub-groups for *Y2K* assessment and remediation purposes. The sub-groups were: FAA; Corporate Safety & Compliance; Operation Control Center (OCC); Delta's

flight attendant scheduling with In-Flight Service; and pilot scheduling with Flight Operations (Flt Ops); Shuttle; and Technical Operations (Tech Ops), which included Delta's Technical Operations Center (TOC), the maintenance repair and overhaul facility in Atlanta. The divisions shown in Table 31 reflect these groupings.

Many of these systems were new at the start of the Year 2000 Program, but others had been in use for a long time. For example, one *Delta Technology* employee who began work at Delta in the late 1980s described his initial assignment as a system development project that supported flight attendant activities. Another informant, a former employee who began at *TransQuest* in the mid-1990s, described his initial assignment as working on changes to a long-established pilot scheduling system, changes which were required because of impending changes to the pilots' contracts. The varying ages of these systems presented different levels of remediation difficulty to the Year 2000 Teams.

The following personnel, shown in Table 32 , had leadership responsibilities in this business area for the Year 2000 Program:[120]

Table 32: Year 2000 Program team in *Operations*

DELTA		*DELTA TECHNOLOGY*
Delta Exec Sponsor: H. Alger, Exec VP – Ops ('97)		
Delta Exec Sponsor: M. Armstrong, Sr VP –Ops ('99)		*Delta Technology* VP: Walter Taylor
Delta Portfolio Owner: J. Poole, Sr VP – IFS		
IT systems not maintained by Delta Technology		*IT systems maintained by Delta Technology*
Corp Safety	Dave Kocsis	*Y2K* Team Leader: John Ruff (9/'97)
IFS	Bob Lederman	Randy McCranie (PMO 11/'97)
Flight Ops	Charlie Bautz/Sue Martin	Eugene Shtern (PMO 11/'97)
OCC/FAA	John Talmadge	*Y2K* PD: Mark Hicks
Shuttle	Moira Kelly	*Y2K* PD: David McGlothin
Tech Ops	Peggy Reagan (12/'97)	

[120] A date beside a name in this table refers to the date of the Delta report that showed the assignment.

As Vice-President - Air Ops Portfolio for *Delta Technology*, Taylor provided leadership for the activities related to the management of IT systems for the *Operations* business area. In addition to this role, Taylor had responsibility for the entire Delta-wide Year 2000 Program. Placing the leadership of the Year 2000 Program in the Air Ops Portfolio was a logical step since this group managed the largest number of systems and lines of code compared to other Portfolio groups. Mac Armstrong was executive sponsor for the Year 2000 Program for *Operations*, and thus had ultimate responsibility for the *Y2K solution* in the business area. As Armstrong was Senior Vice-President – *Operations* for Delta Air Lines, a position that reported to the CEO, the importance of this work is evident. Prior to Armstrong, Harry Alger held the role until he retired.

To ensure that the systems in the *Operations* area would function properly after the year 2000 rollover, as in the other business areas, the *Operations* Year 2000 team took stock of what they had; and from that, they could make decisions for *Y2K solution*. In the inventory and assessment phase, the main activity was to identify and locate all of the systems, and to understand how they interconnected to other systems and to users. The systems were also assessed as to their criticality to operations.[121] Table 33 is a summary of metrics obtained when *Delta Technology* scanned and evaluated the *Operations* systems. The table shows the number of systems, number of programming languages, the lines of code, the number of systems that were waivered, i.e., considered adequate for production after year 2000, and the number of desktop units. Results are indicators of complexity.

[121] A classification (HIGH, MED, or LOW) indicated the critical nature of the system to the functioning of *Operations*.

Table 33: Assessment metrics for systems in *Operations*

NO. OF SYSTEMS HIGH	MED	LOW	NO. OF LANGUAGES	LOC (millions)	NO. WAIVERED SYSTEMS	NO. DESKTOP UNITS
86	59	71	31	25	46	3346

Table 34 lists the languages, the LOC for each language, the numbers of date fields that existed within programming code by language, and the number of date fields affected. These assessments were further indicators of the complexity of the *Operations* systems, and therefore both the importance and the difficulty of making changes to the systems. All of these metrics weighed into decisions for a *Y2K solution*.

Table 34: Programming languages and date fields for systems in *Operations*

LANGUAGE	LOC	DATE FIELDS	DATE FIELDS AFFECTED	PERCENTAGE OF OCCURRENCE
AWK	400			0.00%
Access	207,542			0.00%
Aion DS	312,618			0.00%
Assembler	43,185	299		0.69%
Attachmate	34,890			0.00%
Automator	31,009			0.00%
C	2,031,686	1,355		0.07%
C++	2,035,473			0.00%
COBOL	9,558,412	135,032	14,383	0.15%
Clipper	137,237			0.00%
DCL	55,028	1,182		2.15%
DLPAGER	29,161	1,747		5.99%
Delphi	64,183			0.00%
Exec	26,663			0.00%
Fortran	293,741	22,216		7.56%
Foxpro	35,000			0.00%
GEPR	45,773	242		0.53%
INCL	11,742	67		0.57%
INP	33,482	106		0.32%
JAVA	167,000			0.00%
Natural	7,095,975	624,379		8.80%
Not specified	5,443			0.00%
Oracle Forms	12,630			0.00%
PL/SQL	30,000			0.00%
PLM	13,800			0.00%
Power Builder	216,002			0.00%
Rexx	200			0.00%

Table 34 continued

SAS	127,220	4,604		3.62%
SQL	221,628	2,109		0.95%
Smalltalk	8,000			0.00%
Visual Basic	51,202			0.00%

Besides code remediation or replacement, making no changes to a system was a valid decision. If a system was assessed either to have no date-related issues, or other wise to be an effective, robust system, the team could choose to waiver the system. Table 35 is a list of *Operations* systems that received a waiver, i.e., systems that required no remediation or replacement. Many of the *Operations* systems that were waivered were among the most recent additions to the Portfolio, having been designed and written for the OCC, which is discussed later in this chapter. As another example, Ground Support Equipment (GSE) division had determined in the assessment phase that no failure potential existed in the equipment, even though a comprehensive treatment plan and schedule for stationary GSE equipment had been created. Therefore, remediation of all Ground Support items, other than the Vehicle Management System, was waivered in January 1999.

Table 35: Waivered systems in *Operations*

SYSTEM		LANGUAGE
Operations Waiver - ASD/Off Times Processor	3002	C
Waiver - Cancellation Balancing Application	3003	C++
Operations Waiver - Flight Planning System	3008	C
Operations Waiver - Flight Planning System	3008	C++
Operations Waiver - Graphical Flight Following UNIX	3014	C++
Operations Waiver - Graphical Flight Following Win32	3015	C++
Operations Waiver - Integrated Management Tool	3016	C++
Operations Waiver - Operations Airport Support Information System	3019	C++
Operations Waiver - Pilot Weather Information Display System	3020	C
Operations Waiver - Radio Call Accounting	3021	C
Operations Waiver - Radio Call Accounting	3021	SQL
Operations Waiver - Weather Imagery Display System	3022	C
Operations Waiver - Weather Imagery Display System	3022	Pro-C
Waiver - Workload Management	3024	C++

Table 35 continued

SYSTEM		LANGUAGE
Waiver - Workload Management	3024	UIM/X
Daily Operations Infrastructure: Vics's Program	3036	DOS Basic
DELTA INTRANET HP- Operations Control Center	3040	HTML
Waiver - Diversion Recovery System	3042	C, C++, Java
Waiver - Crew Reroute System	3043	C++, Java
MORPH	4066	Visual Basic
MANUAL INVENTORY TRACKING	4083	Visual Basic
FAT/AD COMPLIANCE TRACKING SYSTEM	4084	Visual Basic
KEY PERFORMANCE INDICATOR TRACKING SYSTEM	4085	Visual Basic
MAINTENCANCE PLANNING & SCHEDULING	4111	C
Operations Portfolio Waiver for TransNet	4166	C++
Operations Portfolio Waiver for TransNet	4166	Visual Basic
FAACOMM SERVER	5015	Clipper/Dbase
FACILITIES INFORMATION TRACKING SYSTEM	5015	Clipper/Dbase
Operations Waiver – PC Backup Weight Data Record	5019	Assembler
Operations Waiver – PC Backup Weight Data Record	5019	C
Operations Waiver – PC Backup Database Download Conversion	5020	C
FAACOMM CLIENT	5027	C
Operations Waiver - Crew Reservation Management System	9006	C
Operations Waiver - Crew Reservation Management System	9006	C++
Operations Waiver - Crew Reservation Management System	9006	Natural
Operations Waiver - Crew Reservation Management System	9006	Pro-C
Operations Waiver - Crew Reservation Management System	9006	SQL
PILOT OFFICE MANAGEMENT	9012	Clipper
Operations Waiver - Safety, Trending and Report System	9017	C++
Operations Waiver - Safety, Trending and Report System	9017	SQL
Operations Waiver - Safety, Trending and Report System	9017	UNIX Script
MEAL ORDERING AND PAYMENT	10003	C++
MEAL ORDERING AND PAYMENT	10003	Java
FLIGHT CANCELLATION REPORT	11002	SQL
Executive Management Tool	11003	SQL
QUALITY ASSURANCE & COMPLIANCE	11030	Foxpro

The next steps, after inventory and assessment, involved system changes—either to remediate the code in a system, to upgrade, or to replace the system altogether. In addition, because of the complex environmental interconnections of the *Operations* area, other activities involved interaction with external parties.

The next sections highlight these activities in four of the *Operations* divisions:

- Operations Control Center,

- In-Flight Service,
- Flight Operations, and
- Technical Operations.

These divisions were selected for greater in-depth attention because they represented high numbers of subdivisions and / or employees, and / or were characterized by high amounts of complexity. In addition, these divisions either were more directly connected with external regulators than the other divisions or otherwise offered unique attributes that provided insight into key study variables. Following discussions of these divisions, the institutional context of the entire *Operations* area is described.

Operations Control Center

The Operations Control Center (OCC), which employed around 350 people at its facility in Atlanta, was a special division of *Operations*. As a $30 million IT project that went live in 1995, the OCC offered specialists from multiple disciplines the tools to perform critical activities related to flight operations.

> Delta's $30 million control center for operations (OCC) opened in late October 1995. From a "bridge" overlooking five jumbo screens, directors watch as computers track the movement of every Delta flight worldwide. Working within earshot of the bridge are meteorologists, traffic planners, mechanics, and reservation specialists (Greising, 1995).

The OCC had been established in order to improve flight operations management for the more than 2,700 flights that Delta's aircraft and crew performed each day. A natural result of better performance of these activities was not only an enhancement to safety, but also a decrease in costly flight delays. The resources of the OCC facility enabled the sophisticated monitoring of all aspects of flight operations: take-offs and landings, weather conditions, and air traffic. This provided better direction for the crews that flew the planes to their national and international destinations. After just over a year

of operations, OCC had paid for itself by cutting nearly 10% from the annual costs that had been attributed to "irregular" flight operations (Caldwell, 1997).

Many of the systems that supported the OCC were brand new in 1996. *TransQuest* developed these systems in-house immediately prior to the official start of the Year 2000 Program, and represented Delta's initial entry into the extensive modernization that was to follow. Individual applications for monitoring and controlling operations involved interactive real-time information processing, and included Aircraft Routing and Control, Graphical Flight-Following, Flight Cancellation Balancing, and Workload Balancing. The Graphical Flight-Following system tracked the status of all Delta flights, and all airports in the U.S. Assisting with these activities were a variety of electronic data feeds, which were obtained by subscription from various outside service organizations, e.g., WSI, Meteorological Office, National Weather Service, etc. The FAA also provided data on a regular basis.

In 1997, *TransQuest* developed and implemented additional systems, such as decision-support tools for flight dispatchers. However, because *TransQuest* had completed development of many of the OCC systems roughly coincidental with the start of the Year 2000 Program, this division did not make any special plans for additional development or replacement of systems during the study period beyond what had been previously designed. Older systems that had buggy code were included with the code remediation project of the Air Ops Portfolio. The new code contained no incidence of the *Y2K* bug and was waivered.

In-Flight Service

> And, of course, you can continue to expect the outstanding service and warm hospitality of Delta's people. We appreciate your support, and we thank you for flying with us (Delta archive, email, 2005).

The In-Flight Service (IFS) division had 18 PDNs and employed around 18,000 flight attendants. Activities of this division focused on services that were performed while onboard the aircraft. These activities related to food and beverage service, cabin servicing, and flight attendants. As mentioned previously, many systems that supported these activities had been in use for a long time, and therefore required remediation of code. An example is the Easy Access Terminal System, which was developed and installed on IBM 286 computers back in 1988.

> Breaking with tradition, instead of CIS people heading systems development teams, departmental managers put in charge of teams. This helped build an interface for the Easy Access system, which runs off two mainframe databases and is used to schedule pilots and flight attendants. The system is mission-critical to Delta with 18,000 people to schedule on a regular rotating basis. Manager of In-Flight Service put together a development team that included programmers, pilots and flight attendants to accomplish user friendly system (Eskow, 1990).

Description of this project also shows that the concept of cross-disciplinary teams was not new to Delta with the Year 2000 Program. Similar to the situation with the older systems in the OCC, the repair process in IFS was accomplished by including the code with the remediation project of the Air Ops Portfolio. Unfortunately, the flight attendant scheduling system was not repaired adequately as part of this process. The system failed to function following rollover to year 2000, which created havoc for a day or two for the passengers who had planned to fly and for the employees called into service to cover the system malfunction. The crew scheduling software was replaced with a COTS product later that year. (“Delta taps Jacada for scheduling,” 2000). The new software was

installed on new hardware that provided access to the airline's crew scheduling systems online.

> More than 27,000 Delta flight crew members view their scheduling assignments via computer terminals in airports serviced by Delta. Jacada's software will be used to make schedules available online through Delta's Intranet and also to graphically enhance the scheduling application, officials said (Ibid.).

Table 36 shows the new system developed for In-Flight Service that had replaced the faulty system.

Table 36: *Y2K solution* in IFS

IN-FLIGHT SERVICE		
Function	**System**	**Vendor**
Crew scheduling		Jacada, Accenture

Flight Operations

Flight Operations (Flight Ops) was the division related to the pilots and the aircraft operation, and included 35 PDNs. Pilots numbered around 8,600 in this division in 1997, a number that had fluctuated somewhat over the previous decade and over the study period because of changing financial conditions in the airline. The division was represented at 180 airport locations, with the main activities at the Hartsfield International Airport and the headquarters campus in Atlanta.

Flight Ops had overall responsibility for flying the aircraft—for organizing the schedules and routes, analyzing flight operations data in order to formulate operational strategies, and managing back-office functions that supported pilots (e.g., training, payroll). Historically, Flight Ops had utilized IT principally to assist with various aspects of flight management, including routing, crew scheduling and training. Table 37 shows the various functions that the division performed.

Table 37: Functional activities in Flight Ops

Aircraft routing, re-routing
Crew records, resources
Customer special assistance program
Flight control, management
Flight Ops communications automation & technology
Flight Ops management, domestic & int'l
Flight Ops publication & manual, services
Flight safety, standards; Operational reliability & control
Engine performance analysis
Radio operators; Dispatch; Meteorology
Pilots, domestic & int'l, trainees
Training, Flight instruction & other, simulator support
Scheduling, crew / training

Table 38 shows the complexity of Flight Ops systems. Flight Ops had 160 systems, the greatest number of systems of all the divisions in *Operations*, which also included the greatest number of high critical systems. Some of the information for this table was not available.

Table 38: Assessment metrics for systems in Flight Ops

NO. OF SYSTEMS			NO. OF LANGUAGES	LOC REMEDIATED	NO. WAIVERED SYSTEMS	NO. DESKTOP UNITS
HIGH	MED	LOW				
68	28	22	n/a	8.5	n/a	293

While the systems experts were busy with assessment and remediation activities, others were interacting with suppliers to understand the level of risk Delta faced, if any, from entities beyond its control boundaries. In the case of Flight Ops, this meant checking aircraft in liaison with manufacturers to get compliance documents.

> Overall, the *Y2K* problem with suppliers was a "trust arrangement"—letters written that indicated compliance, e.g., Boeing certified their planes (Mitchell, 2005).

Table 39 shows the new systems developed for Flight Ops that had replaced systems that were at risk.

Table 39: *Y2K solution* in Flight Ops

Y2K SOLUTION		
Function	**System**	**Vendor**
Flight assignment	Coldstart	Developed with Ilog
Flight-tracking	Total Dispatch	*Delta Technology*

Further assessment involved desktop units, and the possibility to achieve standardization with the Future Vision model. The desktop units were all standardized by replacing with new HP computers with the exception of some that were difficult to resolve prior to the year 2000 rollover, e.g., the pilot/flight attendants' easy access terminal systems (EATS). The software needed replacement both for *Y2K* and because it was an outdated system, but the task was deferred because it was difficult. The software package was unique and functioned in an older operating system environment; and it was not easy to migrate to an Intel Pentium machine. To modify it or rewrite it would have required more resources than *Delta Technology* had available. Consequently, the hardware was patched, but otherwise the systems were left alone for *Y2K*.

Technical Operations

Technical Operations (Tech Ops) was the division that repaired, serviced, and maintained the planes and other flight-related equipment, a $2.0 billion operation. Tech Ops had the largest number of subdivision within *Operations*—191 PDNs, and included over 10,000 employees. Tech Ops was responsible for maintaining a fleet of nearly 600 Delta aircraft and 85 client aircraft. Large subdivisions within Tech Ops included Component Maintenance, Engine Maintenance, and Environment-related activities.

Maintenance facilities in the Tech Ops division were located in nearly 50 U.S. cities and foreign locations. However, its facility in Atlanta, at Hartsfield International Airport, was the oldest. Tech Ops has been operating in Atlanta since 1938, even before

Atlanta became headquarters for Delta. Eight other smaller maintenance bases operated in Chicago, Dallas Fort Worth, and Philadelphia, while other cities did routine aircraft maintenance. The Technical Operations Center (TOC) in Atlanta was the largest such operation in the world, and also one of the world's largest and most modern aircraft restoration facilities.[122] Delta's TOC had been providing this comprehensive range of maintenance support since 1983. Until the completion of the TOC in 1960, Hangar One, and later including Hangar Two, housed all aircraft maintenance for Delta.[123]

The activities within Tech Ops represented by far the greatest amount of diversity of Delta's functional divisions. The Tech Ops specialists understood and managed every part of the very complex aircraft that were in Delta's fleet. Routine maintenance involved periodically dismantling the entire aircraft and reassembling it to make certain that every single part had been accounted for and inspected. Increasingly, various types of application software supported these highly specialized activities. Table 40 summarizes the inventory and assessment results showing that Tech Ops had 122 systems and the Year 2000 Program team remediated 15.5 million LOC, the greatest number of LOCs remediated of all divisions in Operations.

Table 40: Assessment metrics for systems in Tech Ops

NO. OF SYSTEMS			LOC REMEDIATED (millions)	NO. OF LANGUAGES	NO. WAIVERED SYSTEMS	NO. DESKTOP UNITS
HIGH	MED	LOW				
37	29	56	15.5	n/a	n/a	n/a

[122] The sign on the TOC is easy to see from a runway or from the air. It says, "Fly Delta Jets."

[123] Hangar One, located at Delta's Atlanta headquarters campus, is the site for the Air Transport Museum archive, the Museum store (housed in the body of an L-1011), and the Monroe Café.

In addition to code remediation, other remediation included upgrades and replacements for various machine tools, and other similar equipment in the Technical Operations Center (TOC). For example, the scheduled time for Hanger and Power plant tool remediation, as well as shop remediation, was January 1999. (Delta archive, ACT_ITMS.xls, 1999). Tools and diagnostic equipment in Component Maintenance, Engine Maintenance, Environmental Services, and Hangar Maintenance was scheduled for completion in June 1999 (Delta archive, "Delta Year 2000 Program Briefing Book," 1999).

However, the systems that were most critical for their internal functioning, as well as for satisfying the regulators, were the maintenance documentation systems and parts inventory systems. Delta had signed with Digital Equipment (DEC) in 1991 to develop its Technical Operations Publishing System (TOPS) for aircraft maintenance schedules and documentation—the first *online* maintenance information system in the airline industry, which was likely showing its age compared to newer systems.

> TOPS will be deployed on a variety of VAX systems throughout Delta's operations, and includes publishing capabilities based on a database integrated with a Manufacturing Resource Planning system that complies with Air Transportation Association standards. ("DEC puts airline maintenance reports on-line at Delta," 1991).

Around the same time, Delta partnered with Andersen Consulting, reportedly spending between $50 million and $100 million, to develop a LAN-based system called MARC (Maintenance and Rebuild Control) in order to provide Tech Ops personnel with up to date information on aircraft parts.

> Delta has begun converting paper files for record-keeping, inventory and scheduling to an integrated data base co-developed with Andersen Consulting. … Delta is installing local area networks (LANs) at the center to disseminate the automation program to PC users. Delta will use bar-code scanning devices to automatically allocate plane parts, scan documents and sign off on completed repairs (Violino, 1992).

By 1997, however, the parts inventory system was a problem. When performing the inventory and assessments of *Y2K*, Taylor (VP-Air Ops Portfolio) asked TOC management how well parts were being tracked, i.e., how closely did inventory records match reality. “Over 50% was [sic] bad data.” As he investigated how this was happening, he found that users of the inventory system had access to the transaction database; and this access had led to corruption of the data, i.e., problems with data integrity. In addition, the software did not have the cross-functionality (i.e., the comprehensive ERP or supply chain capability) that had become available later in commercial software. Therefore, the decision was made to use Xelus and SAP to extend and improve the processes that they had begun years earlier. Further, the integration of the Tech Ops functions with *Business Support* through the SAP software was expected to produce greater operating efficiency. Tech Ops chose a different application system for inventory management, because it had aviation-specific features that other vendors (esp. SAP) did not offer. Taylor, who became Delta's managing director of MRO process and technology after year 2000, said the company saw a return on its investment in the Xelus software six months after first implementing it (Brown, 2003).

Like other divisions, Tech Ops required liaison with manufacturers to understand the status of the manufacturers’ compliance, in this case regarding aircraft parts. Delta’s Year 2000 Program team sent letters to each of the companies that supplied parts to Tech Ops, and requested written confirmation that the parts were *Y2K* compliant. By January 1999, *Operations* was up to date with requirements for all *Y2K* certifications, i.e., inventory forms, aircraft certifications (Boeing), letters from suppliers, and waiver forms (Delta archive, Act_Itms.xls, 1999).

This completes the functional and resource overview of the four divisions that were highlighted in the *Operations* business area. The next section presents the institutional context of *Operations* in order to assess the reasonableness of the *Y2K solution*.

Institutional context

Activities in the *Operations* area, in existence since the beginning of the crop dusting business, had evolved over time along with the institutionalized regulatory structures that supported the commercial airline industry. Thus, the *Operations* business area had a strong relationship to regulations and other structuring sectoral components relevant to these activities. The following sections describe the cultural character and regulative environment that encompassed all of the divisions in the *Operations* business area, and therefore incorporated the four divisions highlighted above.

Cultural character

The cultural character of the *Operations* business area was the source of the greatest amount of internal tension for Delta. Delta's unions represented dependence and uncertainty, which was evident in labor relations that were continuously threatened by the adversarial posture of the ALPA. Because of the highly visible activities of ALPA within Delta, it was anticipated that Delta's pilots would interact with the *Y2K* teams and possibly influence *Y2K* solutions. Mullin had said in an initial interview that the pilots had picketed ("demonstrated") upon his arrival—his first day at work (L. Mullin, 2004). As an especially noteworthy example of the prominence of the pilots in company activities, part of the collective bargaining agreement with ALPA in 1996 included allowing one pilot representative to attend (but not to vote in) regularly scheduled,

quarterly meetings of the Board of Directors. Beginning with its July 1996 meeting, Delta's Board invited the attendance of an ALPA representative along with three other Delta personnel, the three others representing a new Delta Personnel Board Council. The council was comprised of a representative from each of seven different personnel groups: Airport Customer Service / Cargo; In-Flight Service; Technical Operations; Reservations Sales; Operational Support/Clerical; Field Sales/Sales Support Center; and Supervisory / Administrative. However, neither the council representatives nor the pilot representative had voting rights at Delta's Board meetings. In 1998, once again the pilots tried to negotiate for a voting seat on the Delta Board and were unsuccessful. Then, in what would appear to be retribution against the members of the Delta Board, the pilots' union refused to agree to a pending code-sharing arrangement with United Airlines.

> On April 29, 1998, Delta and United Air Lines, Inc. (United) entered into a marketing alliance agreement (Agreement) pursuant to which the two airlines would engage in code-sharing arrangements, reciprocal frequent flyer programs and other areas of marketing cooperation.
>
> The implementation of the code-sharing aspects of the Agreement is subject to the approval of both companies' pilot unions. In August 1998, Delta's Board of Directors (Board) decided not to grant the request of the Delta pilot union for a voting seat on the Board. Following this decision, the Delta pilot union said it would no longer consider the approval of the code-sharing aspects of the Agreement. As a result, Delta has discontinued consideration of code-sharing arrangements with United (Delta Air Lines, 1998).

The actions of the ALPA thus prevented what might have been a stronger economic position for Delta in the marketplace.[124]

However, even with the disadvantages of the presence of ALPA, Delta enjoyed a financial advantage over its competition because it was 88 percent nonunion while other

---

[124] Note: It seems duplicitous that the pilots criticize the Board for its executive compensation packages when the pilots themselves encourage wage discrimination and unequal benefits between the compensation they receive and that of other personnel. This example revealed their apparent disregard for the efficient operation of the company.

major carriers had many unionized groups (Woods, 2002). The only other group at Delta represented by a union—the Professional Airline Flight-Control Association (PAF-CA)—was the group of 190 employees who worked with air traffic control and ground operations. Other classes of Delta employees had been recruited strongly to join labor unions, but had declined to do so. Table 41 presents the state of Delta's domestic collective bargaining agreements in 1997, and shows the employee groups that were in this situation.[125]

Table 41: Delta's domestic collective bargaining agreements in 1997

PERSONNEL GROUP	UNION	NO. OF EMPLOYEES REPRESENTED	CONTRACT AMENDABLE DATE
Pilots	Airline Pilots Association, International (ALPA)	8,600	May 2, 2000
Flight superintendents	Professional Airline Flight Control Association (PAF-CA)	190	Jan 1, 1999
Flight attendants	Association of Flight Attendants, CWA (AFA-CWA, AFL-CIO)	0	See footnote: [126]
Mechanics	Transport Workers Union of America (TWU)	0	See footnote: [127]
Pilot ground training instructors	Transport Workers Union of America (TWU)	0	See footnote: [128]

Source: Delta Air Lines 1997 Annual Report

The National Mediation Board governed part of the process of unionization as described in the following paragraph:

[125] Note that a zero (0) under the column titled "No. of Employees Represented" means that this employee class was approached by the union, but voted it down.

[126] The flight attendants union continued their success in combating union presence by their votes in 2002.

[127] On December 9, 1997, the National Mediation Board (NMB) dismissed an application filed by the Transport Workers Union of America (TWU) to represent Delta's approximately 10,000 "Fleet Service" employees.

[128] The 107 pilot ground training instructors would join the union in 1999.

> Delta's relations with labor unions in the United States are governed by the Railway Labor Act. Under the Railway Labor Act, a labor union seeking to represent a craft or class of employees is required to file with the National Mediation Board ("NMB") an application alleging a representation dispute, along with authorization cards signed by at least 35% of the employees in that craft or class. The NMB then investigates the dispute and, if it finds the labor union has obtained a sufficient number of authorization cards, will conduct an election to determine whether to certify the labor union as the collective bargaining representative of that craft or class. Under the NMB's usual rules, a labor union will be certified as the representative of the employees in a craft or class only if more than 50% of those employees vote for union representation (Delta Air Lines, 2001).

The Association of Flight Attendants, CWA (AFA-CWA) began a campaign to unionize Delta's flight attendants in 1997, which included opening an association office near Delta headquarters in 1998. According to the NMB, around 5,600 Delta flight attendants, or 29 percent, voted to join the union in 2002, which again did not allow union presence.

> "Delta deeply appreciates the confidence implicit in these election results, which reaffirm the strong relationship between our company and our employees," says Leo Mullin, Delta's chairman and CEO (Woods, 2002).

Like the pilots, Delta's flight attendants were highly paid relative to their counterparts at other carriers; flight attendants earned incomes that ranged from $20,000 to $60,000 annually.

In 1997, the Transport Workers Union had also failed to gain acceptance by the required 35% of Delta ground training personnel. However, after continuing to pursue the goal of representation for this Delta group, they were finally successful in 1999.

> In October 1999, the National Mediation Board certified the election of the Transport Workers Union to represent Delta's 107 pilot ground training instructors (Delta Air Lines, 1999)

Note that no other business area at Delta besides *Operations* had a unionized employee group.

Another aspect of the *Operations* culture was the military training of many of its personnel. Because of the presence of pilots and other influential organization members

who had military experience, military doctrine likely influenced employee performance in *Operations*. Historically, many Delta pilots, mechanics, radio specialists, and ground operations employees had military experience.

The culture in the maintenance division had evolved appreciably over time. The specialized technicians who serviced and repaired sophisticated aircraft had begun as generalists who were the whole source of knowledge about a plane. All they needed were the wrenches and other mechanical instruments that fit the job. Now with data downlink capability, computerized cockpits and data recording instrumentation, a mechanic can know what to repair before the plane lands. In addition, the mechanic must also be increasingly specialized and knowledgeable about the supporting computer-based application systems.

> … "To me," said Delta's technical chief [Ray Valeika, Sr. VP - Technical Operations], "it's a fairly vivid example of how the world of maintenance is changing." In a systems sense, this business has "become much more institutionalized." …Indeed, it's this institutionalization of the field that's led to the unprecedented safety and reliability numbers the industry now enjoys -- a record predicated not on the old idea of hard limits for parts and components, but on a scientific understanding of the architecture of maintenance systems as a whole (Chandler, 2003).

Regulative environment

Government agencies

The activities of the *Operations* divisions were of considerable interest to regulative organizations such as the FAA and others (e.g., EPA, OSHA). Many of the regulations imposed by these agencies had a positive effect on Delta, as well as on the flying public that they were designed to serve. Standards for maintenance, aircraft operating procedures and avionics equipment across the air transportation industry offered the opportunity to develop a resource base that had sustained a safe system for

aircraft operation. Because of the extensive rules disseminated by the FAA especially, it was predicted that the *Y2K* decisions in *Operations* would have been heavily influenced by FAA requirements.

As an example of the influence of FAA rules in the IFS division, Delta's Boeing 737-800 aircraft had an empty area in the rear cabin where seats are normally located. Since FAA rules mandated one flight attendant for every 50 seats, not installing seats in this area limited aircraft capacity to 150 seats, thereby optimizing the number of flight attendants on the aircraft.

Both the U.S. Environmental Protection Agency (EPA) and the FAA had imposed a number of rules in the Technical Operations division related to inspection and maintenance of aircraft. The EPA had the authority to regulate aircraft emissions; therefore, the engines on Delta's aircraft had to comply with applicable EPA standards. The FAA mandated that carriers assume responsibility for an aircraft's airworthiness; and, this rule applied even if the carrier did not perform its own maintenance (Moorman, 2004). In addition, the FAA required that all airlines document all maintenance services, which included tracking every part of a plane and every change made to a plane. In the interest of safety, the FAA required that airlines keep maintenance records for the service life of the aircraft and, that the records be accessible for immediate FAA review. According to FAA rules, if a plane were sold, all records compiled by the seller and any prior owners had to be provided to the buyer. Delta had used software for a number of years to document aircraft repair histories and to manage its parts inventory. However, Delta had led “the list of airlines fined by the FAA for maintenance violations, accruing more than $2 million in penalties from 1986 to 1994” (Light & Tilsner, 1994). It was not

clear whether this was a failure in Delta's IT systems, a failure among system users (mechanics), or if other issues contributed to Delta's poor maintenance record with the FAA.

For several years, growing numbers of substandard or bogus parts had been found in commercial aircraft. In one instance, an engine that was overhauled by a repair station in Turkey lacked FAA approval when it was sold to ValuJet. Many carriers attempting to ward against such circumstances had increased the use of Parts Manufactured Approval (PMA) parts, which were certified by the FAA [under CFR Section 21.303].

While original expectations were that the numerous restrictions imposed by FAA and other agencies would affect Delta's *Y2K* decisions, it turned out that the FAA had its own *Y2K* challenges and thus the relationship between the FAA and airline carriers such as Delta was one of cooperation rather than coercion in *Y2K* activities. Appendix F provides a brief overview of the FAA *Y2K* project.

Industry relationships

> Watts must keep abreast of trends such as increased systems integration. Here he warns that in addition to being integrated, "we also need to make sure these systems are interoperable, meaning that if we fly in Europe, we don't have to have different equipment in Europe than we have in the U.S." (Watts, quoted in Jensen, 2000).[129]

A number of air transportation organizations helped to orchestrate *Y2K* compliance for the industry. These organizations were the same ones that had been instrumental in providing umbrella regulative services since the inception of the industry, i.e., IATA, ATA, and ICAO. A brief example, which related to air traffic control (ATC), gives a sense of the depth of such organizations' involvement in the *Y2K* crisis:

---

[129] Capt. Bill Watts, Delta's Director of Flight Operations and Technical Support.

If the *Y2K* problem resulted in a complete collapse of ground-based ATC while an aircraft was flying, pilots were expected to revert to a "do it yourself" ATC system (Smart, 1999). In-flight Broadcast Procedure (IFBP)—a part of the ICAO *Y2K* regional contingency plans—was to be the primary method used to prevent midair collisions. Using this procedure, pilots would broadcast their flight's crossing times and altitudes on a common radio frequency. Other aircraft would then listen for these broadcasts and minimize potential conflicts by changing their altitude to avoid the other aircraft. As a last resort in the event of the failure of both ATC and IFBP, an on-board Airborne Collision Avoidance System (ACAS), an electronic means for detecting other aircraft, would be used to avoid midair collisions. However, this option was not reliable because in order to detect a potential collision, ACAS required that the threat aircraft be equipped with an ICAO-compliant altitude reporting radar transponder; and, as of 1999, there was no mandatory requirement for aircraft to carry this equipment.

The "trust arrangement" that was enabled by the industry suppliers enabled efficient Y2K compliance activities for Delta. Boeing and aircraft parts manufacturers were critical.

Response assessment

> Walter Taylor, Delta's managing director of MRO process and technology, says the system not only will make the maintenance operation the envy of the industry but will let the airline turn the operation into a profit center by taking in repair and maintenance work for other carriers (Konicki, 2002).
>
> … [With our SAP project] we are developing a core asset at Delta Airlines …. It is absolutely an asset just like one of our aircraft. When we buy an aircraft we make a commitment that we are going to support it. … We have maintenance programs to make sure that asset becomes more efficient and effective as we go. An implementation such as SAP should be no different. (Taylor, quoted in Donoghue, 2002).

Every aspect of the *Y2K solution* in the *Operations* business area shows evidence of rational decision making, with the exception of Tech Ops' choice to lease SAP. Considering the time and cost to implement, as well as the potential consequences if something did not perform as predicted, the SAP decision is questionable. SAP was a complex ERP system. ERP projects are notorious for taking a long time and a lot of money, and sometimes have completely fallen apart. Moreover, the cost and time for training to use SAP following installation has often been far greater than anticipated; and in this case, any mistakes would affect not only Tech Ops, but the finance function as well.

On the other hand, it is reasonable to assume that a single, enterprise-wide computer system is an improvement in efficiency—easier to maintain, and less costly, than an assortment of antiquated systems isolated in different areas of the business. In addition, with the new architecture and common databases already in place, connecting Tech Ops information to it via SAP could provide more reliable demand forecasts for aircraft parts and more efficient and reliable asset management. Furthermore, because all were accessing the same data, the company could reduce complexity, reduce inventory, and decrease the cost of having too many parts on hand. In fact, one informant described his experience in observing the Tech Ops inventory prior to *Y2K* as astonishing.

> Millions of dollars of aircraft parts were just lying around in the shop areas, with no one really knowing what was there.

Another industry source said,

> The cost of having planes idle during unplanned maintenance is around $23,000 per hour, ... And the cost of maintenance is roughly 12% of an airline's total operating expenses. "If [they] can't predict or guarantee that an aircraft is going to be available, then that starts to affect scheduling, availability and utilization" (Burkett, quoted in Brown, 2003, p. 32).

The airline said it specifically chose Xelus for inventory management because it has aviation-specific features that other vendors did not offer. Xelus was performing well to decrease inventory, and decrease associated costs. Therefore, it was easy to understand how the consideration for new inventory software came about.

However, a number of factors had the potential to affect solution choices both during the Year 2000 Program and after it ended. The time constraint of year 2000 was a delimiter for immediate action. The time and resources constraint of *Y2K* meant a delay in dealing with systems installation, similar to the issue of the crew scheduling system described earlier. Therefore, resources were spent for code remediation and other stopgap measures that might have been eliminated without the other demands. Then, Tech Ops initially planned to go live with three of SAP's software modules in 2001, but postponed the implementation until 2002 because of 9/11. Along with Delta's interest in management efficiency, recall that systems development in Tech Ops was driven by institutional requirements. IT systems supported the massive documentation and parts management activities that were required under FAA mandate. However, there was inadequate information related to the SAP solution.

Some had believed that ERP systems were mandatory for managing the maintenance, repair, and overhaul (MRO) supply chain. Maintenance software systems had covered a range of activities from automated planning and scheduling to execution, tracking, and configuration management. In some cases, a solution had directly linked management to the details of activities in line and heavy maintenance and component shops (Moorman, 2004). ERP-like systems had been evolving for decades having been installed in manufacturing environments in the 1960s. However, companies usually

associated with supply-chain software, i2 Technologies and Manugistics, were bypassed because most of the same functionality became available from ERP vendors J.D. Edwards, Oracle, PeopleSoft, and SAP. The ERP vendors could provide improved capabilities in supply-chain technology: integration and collaboration. The MRO function of Tech Ops was very much like a "manufacturing" environment, where operating efficiency related to the availability of parts and an effective process for repairing aircraft. One can envision Fordism principles and Just-in time concepts applying in this environment. However, Delta's Rieder added that

> matters can get complicated when vendors try to apply IT products that are more appropriate for the manufacturing sector to the aviation MRO business.
>
> Unlike manufacturing, which is based on predictable processes, the MRO business is very dynamic, so the challenge is to use the IT system to manage information that is constantly changing in the most efficient manner. We have often found that there is a lack of understanding of the MRO business on the part of the software vendors, which causes implementation problems (Rieder, quoted in Seidenman & Spanovich, 2004).[130]

In fact, the SAP software actually began as a tool for managing the finance function. Did it have other issues related to a possible misfit as well? SAP was being used by other companies to cut costs and to streamline MRO as well as to replace outdated and costly legacy systems. However, this was often a difficult thing to do. Other air carriers had tried to automate their maintenance processes with ERP-like systems and had encountered tremendous difficulties. Nevertheless, Taylor, who oversaw the Tech Ops' SAP installation after year 2000, was convinced that the technology was sound.

> The problem was not with the technology. The systems are proven but hard to implement. Software for any purpose is only as good as the leadership, flexibility of the workforce and [its] implementation (Taylor, quoted in Moorman, 2004).

---

130 Udo Rieder was Delta's Vice President - Engineering and Planning, Technical Operations in 2004.

Some had credited acceptance by the workforce as the major determinant for the overall success of a system. That means if the mechanics on the shop floor failed to interact with the ERP system, then it would be ineffective regardless of the quality of the system itself.

> At Delta, we are replacing legacy systems that are as much as 25 years old and asking people to adapt to the new systems. Often, this involves a difficult cultural change, because the users have learned to use the old systems in ways that are more efficient for them. (Rieder, quoted in Seidenman & Spanovich, 2004).

Others had suggested that the quality of the legacy maintenance data determined its value. Improvements in data standards and practices alone could be significant, but at what cost to get to that point?

Improvements in supply chain management could be huge. With the new systems, Delta planned to continue to service its own aircraft with greater efficiency, but also to bring in more profits through repairing the aircraft of others. Tech Ops tripled its income from repairing other aircraft between 1999 and 2002.

The SAP software implementation began late in 2002, and the comments from Rieder in 2004. With the re-engineering of processes required, the lack of confirmed evidence of fit of the software to the Tech Ops activities, the complete commitment and focus on the installation for years without knowing if it would work, the tremendous expense, etc. the decision was judged as institutional.

Sub-case 2 summary

The *Operations* area performed the main core functions of the airline. The activities of the *Operations* area were complex, and the IT systems that supported them were even more so. Consequently, the divisions in this business area were numerous and many were highly specialized and critical. The analysis of this business area highlighted

the dependency and often-negative influence of the pilots' union, and Delta's dependency on favorable economic conditions to support its financial condition. In contrast to these uncertainties, the external environment of the air transportation industry offered support in effecting the successful *Y2K solution* of *Operations*.

Table 42, Table 43, and Table 43 summarize the information from this sub-case.

Table 42: *Y2K solution* by division in *Operations*

OPERATIONS CONTROL CENTER		
FLIGHT OPERATIONS		
Flight assignment	Coldstart	Developed with Ilog
Flight-tracking	Total Dispatch	*Delta Technology*
TECHNICAL OPERATIONS		
Supply-chain	mySAP	SAP
Supply-chain management	mySAP Business Suite	SAP
Parts management	Xelus Plan, Xelus Extend	Xelus
Technical documentation		Creative Concepts (Gen'l Dynamics subsidiary)
IN-FLIGHT SERVICE		
Crew scheduling		Jacada Accenture

Table 43: Summary metrics in *Operations*

NO. OF EMPLOYEES		
OPERATIONS CONTROL CENTER		350 (1%)
FLIGHT OPERATIONS		8,600 (14%)
IN-FLIGHT SERVICE		18,000+ (29%)
TECHNICAL OPERATIONS		10,000+ (16%)
OTHERS		n/a
TOTAL *OPERATIONS* EMPLOYEES (% total)		~40, 000 (~60%)
NO. OF SUBDIVISIONS		
OPERATIONS CONTROL CENTER		1 (.4%)
FLIGHT OPERATIONS		35 (14%)
IN-FLIGHT SERVICE		18 (7.3%)
TECHNICAL OPERATIONS		191 (77%)
OTHERS		n/a
TOTAL SUBDIVISIONS (% total)		248 (100%)
NATURE OF THE WORK		Unpredictable, complex
NO. OF LOCATIONS		180 airports plus Atlanta
TECHNOLOGY PROFILES	1997	2003
Application systems	216	240
# High/Med/Low critical systems	86/59/71	105/57/78

# Languages	31	
# LOC (millions)	25	
# *Delta Technology* systems	216	240
# Waivered systems	46	
# COTS systems	32	
# Desktop units	3,346	3,346
# Desktop models, original	6	
# Desktop models, solution	3	
Intro computer processing date	Actual date unknown, but prior to 1989	
DOMINANT INDUSTRIES (fields represented)		
FLIGHT OPERATIONS IN-FLIGHT SERVICE TECHNICAL OPERATIONS OTHERS	Aircraft operation Hospitality, catering Aircraft maintenance Flight crew mgmt Corporate safety	
ENVIRONMENT		
GOVERNMENT	FAA, OSHA, EPA, NWS, Customs, DOT, etc	
CULTURAL	Union (ALPA, PCF-CA)	
INDUSTRY	IATA, ATA, ICAO, ACH, ARINC, SITA, etc.	

Table 44: Summary of environmental factors in *Operations*

FACTORS	INSTANCE
Public image	Successful installation of SAP the "envy of the industry"
Belief systems	Delta family, union, military mentality, "trust arrangements"
Existing practices and routines	Shop workers do not need improved software to perform their jobs well, that's for the "geeks" and the "suits." Pilots work best with checklists.
Industry relationships	Boeing, other suppliers, ATA, ATA, ICAO
Regulations	Workplace safety, aircraft safety, FAA
Imitating the solutions of others	"The best run companies run SAP."
Goals	Improve profitability (reduce inventory, costs)
Cost management	Deferring software project to after Y2K, then deferring installation until after 9/11 effects are lessened

Given the *Y2K solution* in *Operations,* its context was examined in order to assess the rationality or institutionality of the decision as an alternative for solving the *Y2K* problem. The solution was assessed as institutional, even though a number of rational influences were noted. Table 45 shows the factors related to the assessment.

Table 45: Factors related to the *response assessment* in *Operations*

OPERATIONAL DEFINITIONS	FACTORS: RELATED TO ***Y2K SOLUTION*** IN ***OPERATIONS***
Institutional model	(*Y2K* Contingency: *Y2K bug*)
CATEGORIES OF EVIDENCE RELATING TO AN INSTITUTIONAL PROCESS	FACTORS THAT CONTRIBUTED TO AN INSTITUTIONAL PROCESS
Cultural • Related to a social fact: perceptions of air transportation, information technology, information security, safety or other value • Cognitive, e.g., military culture • Familiar, comfortable, habitual, e.g., family culture • Related to established relationships, e.g., vendors	1. Conditions in business area and its IT systems: • Systems working but without documentation • Systems woefully out of date • IT employees content with the status quo • Habit of avoiding outside consultants 2. Character of business area environment: • Inadequate conditions in government agency charged with oversight (FAA) 3. Distraction of other business area contingencies: • Financial status • Economic conditions • Competing airlines
CATEGORIES OF EVIDENCE RELATING TO INSTITUTIONAL DECISION-MAKING	FACTORS RELATING TO INSTITUTIONAL DECISION-MAKING IN RESPONSE TO *Y2K*
Regulatory • Requirements for maintaining organizational legitimacy Mimetic (Following the crowd) • Fashionable, popular • Recommended by vendors • Inadequate information about experiences outside organizational boundaries (reporting only successes)	4. U.S. laws, industry regulations: • Industry regulations were focused on coordination & protecting the competitiveness of air transportation, not information security • U.S. govt agencies' systems not *Y2K* compliant • Industry regulations focused on aircraft safety, but inadequately trained for understanding connection to information security. 5. Character of business area environment: • External chaos because of resource limitation • Mixed understanding of the risk • IT products not available in the marketplace that are specifically designed for aircraft maintenance supply chain
Rational-contingency model	
CATEGORIES OF EVIDENCE RELATING TO A RATIONAL PROCESS	FACTORS THAT CONTRIBUTED TO A RATIONAL PROCESS IN IT MANAGEMENT
Goal orientation Actions relating to efficiency and effectiveness Communications related to mission control	1. Leadership: • Acted on the opportunity to improve operations, which made the enterprise more competitive • Stayed actively and personally involved in order to enable best chance for success. 2. Condition of business area and its IT systems: • Process put in place to assure continual assessment with respect to condition of systems and efficiency of performance 3. Responses to business area contingencies: • Management of financial condition (e.g., delaying installations based on budget priorities)

Table 45 continued

CATEGORIES OF EVIDENCE RELATING TO RATIONAL DECISION-MAKING	FACTORS RELATING TO RATIONAL DECISION-MAKING IN RESPONSE TO *Y2K*
Regulatory Requirements for maintaining organizational effectiveness Decision-making criteria • Based on knowledge of systems o *Y2K* compliance o Fit with functional area o Efficiency related to cost, processing, resources, etc. o Security	4. U.S. laws, industry regulations: • Bounding framework of concern by govt/industry rules wherein the condition of aircraft is recognized as vital to safety and national security 6. Organizational leadership: • Knowledgeable about the value of information accuracy and availability • Understood the contribution of IT to the functioning of the organization • Employed personnel with high levels of skills • Adequately responded to security contingencies 6. Character of business area environment: • Personnel resources were adequately aligned with requirements • IT products to serve the needs in Tech Ops were not available in the marketplace, therefore, not supportive of Tech Ops activities.

As the above information indicates, there were both institutional and rational influences that weighed into the *Operations* decisions. The rationality of the decision-making is obvious with respect to the need for greater efficiency in the Tech Ops activities, and the cost savings that could result from a better system than they had. However, the complexity that had developed in the division that came along with the accumulation of features in modern aircraft meant would not be a quick fix to solve the problem. The fact that they had to find bits and pieces of the solution from multiple vendors was evidence of the effort, and the information gathering, required just to do the research and locate systems that could work. Undoubtedly, the desire to take advantage of the DNS architecture along with the complexity of the problem dictated a COTS solution. The cost savings were needed immediately and it would take years to develop such systems in-house, which might have been inferior in the end to those that were evolving in the commercial market.

It seems like a strong possibility that Taylor's recent success with *Y2K*, coupled with his "get it done" attitude (military mentality) and self-confidence, may have made the solution seem feasible. Indeed, the airline might have been better served in the short term to hire a team of IT specialists to work full-time in Tech Ops to make better use of what they already had. That would have given the ERP vendors time to develop specific solutions for an airline technical operations environment. One can observe that Delta's history includes a number of "firsts," and that Delta likely had become accustomed to being an early adopter of technology. In this case, "early" carried far too much risk.

Sub-case 3: *Business Support*

> Delta has had extensive turnover at the top in recent months as it struggles to regain its financial footing, and analysts and investors said the role of the CFO there is vital (Reuters News Service, 2004).
>
> Delta Air Lines has undertaken aggressive IT projects which power the airline from almost every angle. In addition to going live with a massive database and infrastructure for sharing real-time information that spans a large part of the Delta enterprise, the airline's finance function and MRO have implemented SAP over the past two years and continue to roll out new releases. (Murray, 2002, p. 1).

Y2K solution

The Finance division replaced almost all of their systems, but not until after year 2000. Delta implemented two modules from software maker SAP, which connected users via the DNS across the supply chain, financial reporting, and human-resources functions. The SAP software provided access to various data and processes that changed the way the business was run. For example, in the early to mid-1990s, various Delta managers were authorized to write checks. SAP financial software centralizes check-writing. On Target Technologies then redesigned an existing application to analyze Delta's SAP data in a timelier fashion. The new system was able to access daily information from SAP as well as from many other concurrently online systems, to produce accurate consolidations of business intelligence data, providing financial reporting, forecasting and planning capability. However, one of the Delta employees interviewed stated that *Y2K* repairs had created information security problems for *Business Support*. Table 46 shows the new systems.

Table 46: *Y2K solution* in *Business Support*

BUSINESS SUPPORT		
Function	**System**	**Vendor**
Financial management	mySAP, Business Suite	SAP

Table 46 continued

Business analytics (financial reporting, forecasting, and planning functionality)	Essbase, Enterprise Miner, Brio	Hyperion, SAS, Brio
Supply-chain management	mySAP Business Suite	SAP

Functional and resource overview

The *Business Support* area was charged with hiring the workers, paying the taxes, accounting for revenue and expenditures, and with purchasing, planning, and budgeting for future operations. These functions are common to most commercial enterprises; therefore, the regulative environment of the *Business Support* area of Delta had evolved over time and encompassed similar functions in all U.S. enterprises. In particular, the finance and accounting service functions had been a core part of Delta's profit making enterprise over the 75 years of its existence, and the IT systems had evolved along with the accounting profession and their associated rules. The Chief Financial Officer (CFO) at Delta was responsible for IT.

> In many companies responsibility for implementing and maintaining electronic data processing equipment remained under the auspices of the accounting or finance department because they were the earliest users of the new technology (Gale, 1968, p. 46; Gallagher, 1961, p. 28).

Table 47 shows the complexity and scope of *Business Support* activities as evidenced by 127 department numbers. The numbers of *Business Support* locations could not be determined, but a large part of its operation took place at Delta's Atlanta headquarters.

Table 47: No. of divisions and no. of locations in *Business Support*

DIVISION	PDNS	NO. OF LOCATIONS
Government, Public and Community Affairs	3	
Investor Relations	1	
Corp Communications	1	
Capital Markets, Treasury	2	

Table 47 continued

Financial Analysis, Financial Planning, Financial Reporting	3	
Finance Business Support – Other, Printing & Mailing Svcs	2	
Accounting, Corporate Tax	2	
Corporate Security	1	
Legal	1	
HR		
Purchasing		
Properties & Facilities	1	
Museum	1	
Internal Audit (outsourced), Risk Management	2	
Delta Staffing Services, changed to DGS (Delta Global Services)	1	
Executive Support	1	
TOTAL	127	Atlanta +

Table 48 provides further description of this business area in the activities in divisions and the application systems that supported them.

Table 48: Functional divisions and systems in *Business Support*

DIVISION	SUBDIVISION	APPLICATION SYSTEMS
Financial management		
	Accounting	Payroll; Accounts payable; Accounts receivable; General ledger maintenance; Fixed asset accounting
	Financial Analysis	Capital budgeting models; ROI models
	Financial Planning	Annual budgeting
	Financial Reporting	Preparation of financial statements for management, SEC, annual reports, internal and external auditors
	Internal Audit	sampling models
	Treasury	Cash management; similar to capital markets; short term investments tracking
	Capital Markets	Tracking bond prices/yields; bank loans
	Corporate Planning	
	Corporate Tax	Tax preparation
	Risk Management	Insurance claims; policy data bases;
Human resource management		
	Personnel	General employee database mgmt; performance evaluations; surveys of managers satisfaction with employees
	Delta Staffing Services	Résumé management; job postings; performance evaluations of temps; surveys' of managers satisfaction with temps;
Legal		
		Case databases, internal lawyer scheduling; databases regarding communication with outside counsel, contracts and laws regarding partnerships, international, etc.

Table 48 continued

External affairs		
	Gov/Public Affairs	Mgmt of databases of key officials by gov't entity; key pending legislation; text from positions taken by supporters and opponents; text documenting key meetings and conversations; scheduled meetings
	Community Affairs	Managing databases of employee participation on civic boards and volunteer hours donated to the community; target organizations to become close to because of key customer involvement with those organizations; scheduled events for the company to attend/support; list of charitable contributions
	Corporate Communications	Managing databases of media services and key reporters; text of news releases; possibly similar use of governmental affairs for emergency contact and similar to investor relations to notify shareholders of key info
	Investor Relations	Management of shareholder database; communication records with shareholders; stock transfers; stockholder meeting activities, schedules
Facilities management		
	Properties & Facilities	Managing asset inventory; maintenance records; depreciation calculations to tie into the financial systems; asset records
	Corporate Security	Staffing schedules for security officers; incident reports; employee databases similar to HR
	Museum	Inventory of contents; staffing schedules
Business services		
	Purchasing	Arranges for purchases for all business areas, including negotiating agreements, contracts, and warranties.
	Printing & Mailing Services	Graphics arts software; data bases; postage

The following personnel shown in Table 49 had leadership responsibilities in the *Business Support* area for the Year 2000 Program.

Table 49: Year 2000 Program team in *Business Support*

DELTA	*DELTA TECHNOLOGY*
Delta Exec Sponsor: R. Coleman, Exec VP - HR ('97)	
Delta Exec Sponsor: W. Jenson, Sr VP – CFO ('98)	*Delta Technology* VP: D. Pittman
IT systems not maintained by Delta Technology	*IT systems maintained by Delta Technology*
	Y2K PD: Stephanie Hill

The top decision-maker on the *Business Support* Year 2000 Team changed a number of times over the study period. The first Executive Sponsor was Delta's executive in charge of Human Resources (HR), but by 1998, the responsibility had been reassigned to the new CFO, Warren Jenson. Delta had four CFOs in four years. Jenson had replaced Tom Roeck, a Delta veteran, who left in 1997 when Mullin came aboard as new CEO, which was not an unusual happening. Then two CFOs (Warren Jenson, and after him, Ed West) left Delta to work for dot-coms. The fourth CFO was Michele Burns, who joined Delta in 1999 and became CFO in 2000. Burns resigned in April 2004, along with Mullin and a number of other management-level employees—the year before Delta declared bankruptcy. She was the third to leave in 2004, following the departures of Fred Reid (President and COO) and Robert Coleman (Exec VP-HR) (Reuters News Service, 2004).

Table 50 is a summary of metrics obtained when *Delta Technology* assessed the *Business Support* systems.

Table 50: Assessment metrics for systems in *Business Support*

NO. OF SYSTEMS			NO. OF LANGUAGES	LOC (millions)	NO. WAIVERED SYSTEMS	NO. DESKTOP UNITS
HIGH	MED	LOW				
19	53	107	16	12	17	~600

Table 51 lists the languages, the LOC for each language, the numbers of date fields that existed within programming code by language, and the number of date fields affected. These assessments provided evidence of both the criticality and the complexity of the systems, and therefore both the importance and the difficulty of making changes to the systems.

Table 51: Programming languages and date fields for systems in *Business Support*

LANGUAGE	LOC	DATE FIELDS	DATE FIELDS AFFECTED	PERCENTAGE OF OCCURRENCE
Access	9,100			0.00%
Assembler	199,115	909		0.46%
Attachmate	85,435			0.00%
C	1,992,141			0.00%
COBOL	3,425,350	80,087	18,149	0.53%
Clipper	40,311			0.00%
Exec	1,174	31		2.64%
Fortran	73			0.00%
Integra	248,136			0.00%
Natural	319,128	36,935		11.57%
Not specified	341,918			0.00%
ReportBuilder	126,771	17,373		13.70%
SAS	154,164	1,665		1.08%
SQL	160,953			0.00%
TGS	367,577	14,823		4.03%
Visual Basic	230			0.00%

Table 52 shows the systems that received a waiver, i.e., systems that required no remediation or replacement.

Table 52: Waivered systems in *Business Support*

Pass Bureau - Waiver	2012	Access
Project Planning Tool	2042	Pro-C
Business Support Waiver - New Hire Database	2044	Waivered: System not in use
TQPants	2052	SQL
TQPants	2052	Visual Basic
Project Tracking System	2054	Access
Business Support Waiver - New Hires Information System - Early Warning System	2056	Access
Corporate Records Contact Tracking System	5012	Clipper/Dbase
A&CA Contact Viewing System	5013	Clipper/Dbase
A&CA Contact Tracking System	5014	Clipper/Dbase
FACILITIES TRACKING INFORMATION SYSTEM	5015	Clipper/Dbase
Playtypus	8040	Not specified
Waiver Employment Verification System	8047	SAS
Personnel Data Warehouse	8087	Access
Conference Room Scheduler	11001	Clipper/Dbase
Business Support Waiver - Time Keeping (Paradox) (Delta)	11026	COTS-Not specified
Business Support Waiver - International Bank Reconcile (Delta)	11032	Not specified

Institutional context

Cultural character

While the *Business Support* area was not connected to the military culture, the family culture was strongly related to this area, since the benefits that came from seniority were accounted for in this division. There was also a strong association with information technology, since IT systems were readily available for assisting with the activities in this area long before other specialty areas. The Finance area had been called the "nerve center" of the organization since the profit and loss accounting would relate to organizational survival. There was tension in the family in this area at Delta immediately prior to the executive changes of 1997.

> Of all the CFOs he has known at Delta, "I put Tom at the top," says Jesse Hill Jr., chairman of the audit committee and now Delta's senior director. "He has done an outstanding job," especially in reducing debt and formulating an aggressive cost structure to fight the competitive war with Southwest Airlines Co. and other lower-cost carriers. "The finance department has to be the nerve center" for such strategies, says Hill, a retired life insurance executive. "At every meeting, the principal report, other than the comments of the CEO, comes from Tom Roeck; he's the one we focus on."
>
> Interviews with recently departed Delta managers, including some who worked in finance, paint a picture of a headquarters where Roeck was often excluded from Allen's inner circle. As a result, Roeck sometimes found himself treated badly by other top-level executives closer to Allen; finance department members formed mixed allegiances; and the role of finance at the airline suffered (Harris, 1997).

Regulative environment

Government agencies

The government regulators that were most concerned with *Business Support* were the SEC, the IRS, the DOT, and DOJ. The company followed generally accepted accounting principles (GAAP). Delta's unconsolidated operating revenue and operating income by geographic region were reported to the DOT (which differed from operating

revenue and operating income (loss) reported under GAAP). Performance results for Delta's transatlantic operations were based on allocations in accordance with requirements of the DOT. Delta's legal division took its direction from regulations related to the air transportation industry but also the Department of Justice (DOJ).

Industry relationships

The industry regulators that were most concerned with *Business Support* were the independent auditors, and the professional bodies associated with the accounting, legal and justice systems. For example, Arthur Andersen & Co served as independent auditors for Delta until 2002, thereafter, Deloitte & Touche. Various rules associated with the Financial Accounting Standards Board (FASB) applied to their activities, which were required under the rules of the SEC. The AICPA and the American Bar Association (ABA) were interpreters of IRS regulations and other business rules. These and other professional associations related to the *Business Support* divisions. The Purchasing group handled contracts with all of the contractors/suppliers for Cargo. (Delta archive, Defnote1.doc). Each City Ticket Office (CTO) had agreements with local banks.

Table 53: Year 2000 Program snapshots – *Business Support*

DATE	KEY EVENT	PLAYERS	COMMENT
1990-1996	Finance reengineering	Andersen Consulting	Around 500 people (AC & DL) performed a complete redesign and implementation of the processes and IT systems in the Finance area.
Nov/1997	CFO retired	Tom Roeck	Roeck was highly regarded by Delta's Board. Had been at Delta for 8 years. Arrival of CEO Mullin implicated in his departure.
	CFO	Warren Jensen	Jensen left following unfortunate seat assignment for his family that meant deplaning first class customers.
	CFO	Ed West	Resigned
Aug/2000	CFO	Michele Burns	Burns was hired in Jan 1999 from AA&Co tax dept. Departure to Mirant came when execs were being asked to give up their executive salaries and other perks.
May/2004	New CFO	Michael Palumbo	Palumbo was a Grinstein colleague at Western Airlines.

Response assessment

Within the context and conditions of *Business Support*, the Y2K solution decision is rational. *Business Support*, specifically the finance function, had re-engineered processes over a six year period in anticipation of the DNS architecture becoming available. *Y2K* delayed them in doing this. The SAP installation was the opportunity to integrate the processes into the IT systems in a more efficient manner. However, all of these processes were based on conformance with various rules for accounting and reporting of organization activities. The regulative processes that govern these activities are viewed differently depending on a rational or institutional perspective. For example, from a rational perspective an organization assesses tax regulations with respect to their consequences to profitability. From an institutional perspective, such regulations are a product of a values-oriented social system, where a larger societal goal may not respect the consequences to an individual organization. Therefore, tax consulting is more than just compliance reporting. It is lawyers and accountants trying to interpret tax regulations for the benefit of their clients. Either a more aggressive or a more conservative interpretation can emerge that is different from what the lawmakers intended.

However, the institutional mechanisms that supported the SAP installation had other dimensions, the marketplace competition, increased complexity of IT systems that accommodated an increasingly complex regulative environment, and the increased complexity of Delta's partnership activities. Therefore, an institutional perspective focuses on the popularity and visibility of SAP. This product had become the dominant COTS solution for the finance organizations of many large companies. The finance functions were institutionalized across enterprises regardless of the particular business

activities of an organization. The functionality of the SAP suite of financial applications were based on a long history of institutional "best practices," as dictated by FASB reporting and commonly accepted internal control procedures. This made the SAP selection for the finance area a rational choice when compared to an in-house custom development approach. The rational choice was made within an environment of institutional practices. The rationality is tied to its increased efficiency and effectiveness as a tool for reducing complexity in accounting for the operations of a very complex organization. In addition, Delta demonstrated rational cost management by adapting the overhaul to fit their financial condition. Delta deferred projects that would take more than a year to pay off (like new HR systems).

Sub-case 3 summary

The *Business Support* area was the site for human resource functions, tax preparation and payment, accounting for revenue and expenditures, and with purchasing, planning, and budgeting for future operations.

Table 54 and Table 55 summarize the *Y2K solution*, and the environmental conditions in the *Business Support* area, respectively.

Table 54: *Y2K Solution* in *Business Support*

BUSINESS SUPPORT		
Function	**System**	**Vendor**
Financial management	mySAP, Business Suite	SAP
Business analytics	Essbase, Enterprise Miner, Brio	Hyperion, SAS, Brio
Supply-chain management	mySAP Business Suite	SAP

Table 55: Summary metrics in *Business Support*

TOTAL *BUSINESS SUPPORT* EMPLOYEES (% total)	3,500 (%)	
TOTAL SUBDIVISIONS (% total)	127 (%)	
NATURE OF WORK	Routine	
LOCATIONS	Atlanta	
TECHNOLOGY PROFILES	1997	2003
Application systems	179	218
# High/Med/Low critical systems	19/53/107	20/56/142
# Languages	16	
# LOC	12	
# *Delta Technology* systems		
# Waivered systems	17	
# COTS systems	111	
# Desktop units	585	
# Desktop models, original	51	
# Desktop models, solution	2	
DOMINANT INDUSTRIES (fields represented)		
	Investor relations Accounting Auditing Communications Facilities Mgmt Finance HR Legal Tax	
ENVIRONMENT		
GOVERNMENT	SEC, OSHA, IRS, DOT, DOJ	
CULTURAL	Non-union	
INDUSTRY	ABA, AICPA, FASB, local banks	

Table 56: Summary of environmental factors in *Business Support*

FACTORS	INSTANCE
Public image	"The best run companies use SAP"
Belief systems	Business ethics, strength of the regulatory system
Existing practices and routines	Highly supported by IT systems, comfortable with standard suites of business applications
Industry relationships	
Regulations	Tax, HR, Accounting, Securities: IRS, FASB, SEC
Mimesis	"Airport of the Future," SAP
Goals	Improve centralized processes for accounting
Cost management	Reduce complexity of operations

The *Y2K solution* in *Business Support* was examined in light of its context in order to assess its rationality or institutionality as an alternative for solving the *Y2K*

problem. Given the conditions of the *Business Support* systems and other requirements, the solution was considered rational. Table 57 shows the factors related to the assessment.

Table 57: Factors related to the response assessment in *Business Support*

OPERATIONAL DEFINITIONS	FACTORS: RELATED TO *Y2K SOLUTION* IN AIRPORT CUSTOMER SERVICE
Institutional model	(*Y2K* Contingency: *Y2K bug*)
CATEGORIES OF EVIDENCE RELATING TO AN INSTITUTIONAL PROCESS	FACTORS THAT CONTRIBUTED TO AN INSTITUTIONAL PROCESS
Cultural • Related to a social fact: perceptions of air transportation, information technology, information security, safety or other value • Cognitive, e.g., military culture • Familiar, comfortable, habitual, e.g., family culture • Related to established relationships, e.g., vendors	6. Conditions in business area and its IT systems: • Systems not entirely integrated across business areas • IT employees familiar with IT systems • Familiar with the presence of consultants 7. Character of business area environment: • Most advanced in mechanisms because of history 8. Distraction of other business area contingencies: • Financial status • Economic conditions
CATEGORIES OF EVIDENCE RELATING TO INSTITUTIONAL DECISION-MAKING	FACTORS RELATING TO INSTITUTIONAL DECISION-MAKING IN RESPONSE TO *Y2K*
Regulatory • Requirements for maintaining organizational legitimacy Mimetic (Following the crowd) • Fashionable, popular • Recommended by vendors • Inadequate information about experiences outside organizational boundaries (reporting only successes)	9. U.S. laws, industry regulations: • Industry regulations were focused on protecting the investor and the regulators • U.S. govt agencies' systems not *Y2K* compliant • Industry regulations focused on passenger screening after 9/11, but inadequate solutions. • Industry regulations linked to intelligence gathering—a public concern strongly related to privacy, but not linked to information security 10. Character of business area environment: • External chaos because of time limitation • Strong understanding of risk, therefore reluctant to get involved • Strong, reliable IT products in the marketplace

Table 57 continued

OPERATIONAL DEFINITIONS	FACTORS: RELATED TO *Y2K SOLUTION* IN AIRPORT CUSTOMER SERVICE
Rational-contingency model	
CATEGORIES OF EVIDENCE RELATING TO A RATIONAL PROCESS	FACTORS THAT CONTRIBUTE TO A RATIONAL PROCESS IN IT MANAGEMENT
Goal orientation Actions relating to efficiency and effectiveness Communications related to mission control	4. Organizational leadership: • Acted on the opportunity to improve operations, which made the enterprise more competitive • Leadership turnover, not actively involved in order to insure success with systems implementation. 5. Condition of business area and its IT systems: • Process put in place to assure continual assessment with respect to condition of systems and efficiency of performance 6. Responses to business area contingencies: • Good management of financial condition (e.g., delaying Finance systems based on budget priorities)
CATEGORIES OF EVIDENCE RELATING TO RATIONAL DECISION-MAKING	FACTORS RELATING TO RATIONAL DECISION-MAKING IN RESPONSE TO *Y2K*
Regulatory Requirements for maintaining organizational effectiveness Decision-making criteria • Based on knowledge of systems o *Y2K* compliance o Fit with functional area o Efficiency related to cost, processing, resources, etc. o Security	7. U.S. laws, industry regulations: • Even though limited and late in coming, a bounding framework of concern by govt/industry rules wherein the condition of IT systems was recognized as vital to safety and national security 8. Organizational leadership: • Knowledgeable about the value of information accuracy and availability • Understood the contribution of IT to the functioning of the organization • Employed personnel with high levels of skills • Adequately responded to security contingencies 7. Character of business area environment: • Personnel resources were adequately aligned with requirements • IT products to serve the needs in *Business Support* were available in the marketplace

The fact that the institutionalized environment of *Business Support*, principally the finance area, has changed little over the years and that computer technology has been used to support the function since practically the beginning of electronic computing, the market place has developed simultaneously. In fact, the evolution of the ERP systems has kept pace with the leading edge of network computing innovation. This is evidenced by the product offered by companies, such as SAP. Therefore, the move to the new architecture of Delta was supportive of the addition of such a software package in the

finance division. The compatibility of the new software with the existing software, even though connected with the DNS system, enabled a familiar activity on the part of the users and required little change with regard to their routines.

In sum, the *Business Support* area is supportive of rational-institutional compatibility. They had the most complete information, clear choices among products, proven products in the marketplace, and supported the future vision of modernization. Thus, it is not surprising that their decision-making regarding *Y2K* solutions was rational.

Sub-case 4: *Revenue*

Y2K solution

Besides the assessment, code remediation and other modernization activities, the *Revenue* business area chose to install new applications for revenue management.

Table 58: *Y2K solution* in *Revenue*

REVENUE		
Function	**System**	**Vendor**
Revenue optimization	NetWORKS Airline Revenue Optimizer	Manugistics Accenture
Flight network analysis	Planet	Kiehl Hendrickson Group
Sales automation	BaanFrontOffice	Baan

The principal additions in the *Revenue* business area were implementation of a system called Planet for analyzing an airline flight network, and a system called NetWORKS for optimizing revenue. The Planet System used state-of-the-art technology to forecast the market share, revenue and profitability consequences arising from assumed changes in airline flight networks, demand conditions, competitive structure, and other market dynamics. Kiehl Hendrickson Group (KHG) had previously installed Planet for such customers as Trans World Airlines (TWA), Comair, Frontier Airlines, Atlantic Coast Airlines, Bombardier Aerospace, the U.S. Department of Transportation, and others ("Delta Air Lines installs new route planning system," 2000). NetWORKS was a product from Manugistics[131] that calculated seat pricing, using a number of variables that were changing continuously. *Revenue* tied this into the DNS where real-time data was available from moment to moment, and using this software, they could automatically

[131] Manugistics was a software company well-known for its cross-functional business applications.

generate pricing options especially for web based seat reservations systems. BaanFrontOffice was chosen for sales automation.

Functional and resource overview

The *Revenue* business area comprised the business areas of Delta that performed functions related to income production, i.e., marketing and sales. At the beginning of the study period, *Revenue* had over 10,000 employees in sales and distribution, which represented over 15% of the Delta organization. The scope and complexity of the *Revenue* business area was indicated by its 62 divisions, which include Alliance marketing Consumer Marketing, Delta Express, Europe-Asia, Marketing Administration, Marketing Development, Revenue Accounting, and Sales. Information regarding numbers of locations was not available. See Table 59. The Revenue Accounting division was responsible for accurate and timely accounting and reporting of passenger and alliance revenues, receivables, taxes, commissions, and related flight statistics information.

Table 59: Number of divisions and no. of locations in *Revenue*

DIVISION	PDNS	NO. OF LOCATIONS
Alliance marketing	2	
Consumer marketing		
Delta Express	1	
Europe-Asia		
Marketing Administration	1	
Marketing Development	5	
Market Analysis		
Schedules		
Pricing/Revenue Management		
Marketing Executive	1	Atlanta Campus
Revenue Accounting	11	
Sales (passenger)	27	~195,(Atlanta Campus, Worldwide)
TOTAL	62	~195,(Atlanta Campus, Worldwide)

The following personnel shown in Table 60 had leadership responsibilities in this business area for the Year 2000 Program:

Table 60: Year 2000 Program team in *Revenue*

DELTA	*DELTA TECHNOLOGY*
Delta Exec Sponsor: F. Reid, Exec VP & CMO – *Revenue* ('98)	*Delta Technology* VP: Mark Sohl
Delta Portfolio Owner: V. Caminiti, Sr VP – Sales & Distribution Planning	
Delta Portfolio Manager: Larry Beck (5/'98)	
IT systems not maintained by Delta Technology	*IT systems maintained by Delta Technology*
Over 200 systems (CRS, others)	*Y2K* Team Leader: Steve Cooper (9/'97)
	Y2K PD: Steve Smith

Results of the first phase, the inventory and assessment actions, are shown in Table 61 and Table 62, which indicates the level of complexity that existed in the systems in this business area. The inventory identified the systems; the assessment phase classified them based on their criticality to the functioning of the *Revenue* business area.

Migration planning was the phase where the team confirmed action plans. In the code remediation phase, the code that had been previously identified as containing the *Y2K* bug was sent to one of two outside organizations to be cleaned. In the desktop renewal phase, desktop units were replaced with the standard models identified by particular division. The other data shown in Table 61 are the number of programming languages represented, the lines of code (LOC) requiring remediation to eliminate the *Y2K* vulnerability, the number of waivered systems, and the number of desktop units assigned to the area.

Table 61: Assessment metrics for systems in *Revenue*

NO. OF SYSTEMS HIGH	MED	LOW	NO. OF LANGUAGES	LOC (millions)	NO. WAIVERED SYSTEMS	NO. DESKTOP UNITS
24	77	1	16	10	33	629

Table 62: Programming languages and date fields for systems in *Revenue*

LANGUAGE	LOC	DATE FIELDS	DATE FIELDS AFFECTED	PERCENTAGE OF OCCURRENCE
Access	8,000			0.00%
Assembler	49,509	1,194		2.41%
C	1,410,831			0.00%
C++	838,908			0.00%
COBOL	2,079,709	45,216	6,969	0.34%
Delta Term	2,500			0.00%
Easytrieve	1,003,443			0.00%
Exec	13,025	267		2.05%
Fortran	117,064	2,089		1.78%
LISP (AI)	230,394			0.00%
Natural	1,570,999	157,523		10.03%
Not specified	707,478			0.00%
Rexx	296	6		2.03%
SAS	701,038	60		0.01%
SQL	573,177			0.00%
Visual C++	45,000			0.00%

Designed by IBM and installed in 1964, Delta's Deltamatic flight reservation system was one of the first computer-based systems for airline reservation management that performed information processing in real-time.[132] This type of processing was developed for the U.S. military where "real-time" information was necessary to calculate projected trajectories for missiles. Earlier systems had provided fast access to flight information but had not been interactive. They could retrieve information quickly, but entering the information was a separate action. Before that, reservations still had to be recorded by hand and calls placed to airlines to confirm availability. These specialized

[132] American Airline's SABRE (Semi-Automatic Business-Related Environment) reservation system was developed by IBM and implemented in 1961. See Smithsonian National Museum of American History, Terminal Interchange from PANAMAC Airlines Reservation System.

systems developed into competitive tools for mining passenger information, along with the data from flights to use in automated pricing algorithms.

The *Revenue* business area chose to install such new applications to improve the pricing of airline seats. Accenture assisted in the custom installation. Prior to the DNS installation, detailed revenue information had not been available. The actual numbers that corresponded to various variables in seat pricing algorithms were not available; therefore, statistical values were being used. Reporting was done based on sampling, and extrapolations had been used to determine revenue. "Statistically the numbers were good, but they did not have the actual values on a flight by flight basis" (J. McMillan, 2006, Sep 29, interview by author, Atlanta, GA). Calculations were performed based on averaging of values within the constraints of aircraft, route, configuration of class, i.e. first class or economy, demand as it materialized toward flight departure date and time. The calculations for making revenue projections and pricing models were complex. No manual calculations could have substituted for computer-based processing for this application. This project began in the '99-'00 timeframe and they were still working on this at least until 2004, having all projects shut down and restarting following 9/11.

In 1999, Delta signed a $9 million, 1,200-user contract with Baan Co. to replace a 4-year old in-house sales-automation system with BaanFrontOffice software. This software allowed Delta's sales force to mine the company's customer records and find the best and overlooked sales opportunities through integrated data models.

> "The primary purpose of turning to this now is Y2K," said Mark Sohl, a VP at DT. The airline will spend approximately $390m building new revenue-management and sales force systems, updating its scheduling system, shoring up its pricing system and installing intranet training systems and a boundary-breaking middleware system to track passengers and flights (Deck & Stedman, 1999).

The in-house system had *Y2K* issues, so the team chose replacement rather than remediation for the old code. Delta's installation was much larger than the typical Baan installation of 300 to 600 end users.

Institutional context

Cultural character

After 1978, the Delta internal organization, as well as Delta's sectoral environment, experienced a number of changes, particularly in marketing, in response to the changes brought about by deregulation. Marketing began to play a strategic role in the company and in the air transportation industry in general, more so than before. As an example, in 1981 Delta formed Epsilon Trading Corporation, a computerized marketing subsidiary, to coordinate and sell more passenger seats on all Delta flights. In 1982, Delta formed Datas Incorporated, another computerized marketing subsidiary. The competitive environment created a requirement for computer processing, and even though Delta had been a follower, rather than a leader, in this environment, the employees were accustomed to the requirement for computer use. The DNS and the investments made during Y2K enabled them to enjoy a role as leader.

Regulative environment

Government agencies

The department of Justice was concerned with the use of computer systems to enable competitive advantage. The issues related to using such information in violation of privacy are in the forefront following 9/11.

Industry relationships

Industry relationships have historically associated with travel agents and other vendors that connect with revenue management and sales activities. This has been greatly diminished by the introduction of the Internet and online reservations capabilities.

Response assessment

Taking advantage of the DNS architecture to enhance marketing and sales capability is a rational decision. Further, these systems reduced cost and complexity, and enabled predictability of operations. They could not have generated the same information in-house for the same cost without writing code with sophisticated and dynamic processing capability. Taking advantage of historical flight information that was captured by the DNS automatically allowed the optimal efficiency of aircraft utilization without adding any addition resources for the effort. The result was positive consequences for both efficiency and effectiveness.

Sub-case 4 summary

The *Revenue* business area of Delta served as Sub-case 4. The sub-case included a description of its *Y2K* compliance response (*Y2K solution*) and the context for this action provided both by the *Revenue* business area and by its sectoral environment. The *Y2K solution* included remediating code in existing high critical systems in order to remove the *Y2K* vulnerability, replacing the airline ticket pricing system, and enhancing the automation of its sales systems.

Table 63: *Y2K solution* in *Revenue*

REVENUE		
Function	**System**	**Vendor**
Revenue optimization	NetWORKS Airline Revenue Optimizer	Manugistics
Sales-automation system	BaanFrontOffice	Baan Co.
Flight network analysis	Planet	Kiehl Hendrickson Group

Table 64: Summary metrics in *Revenue*

TOTAL *REVENUE* EMPLOYEES (% total)		~10, 000 (~15%)
SUBDIVISIONS		
TOTAL SUBDIVISIONS (% total)		62 (%)
NATURE OF WORK		dynamic
LOCATIONS		Atlanta
TECHNOLOGY PROFILES	1997	2003
Application systems	102	122
# High/Med/Low critical systems	24/77/1	26/84/12
# Languages	16	
# LOC	10	
# *Delta Technology* systems	102	
# Waivered systems	33	
# Desktop units	529	
# Desktop models, original	13	
# Desktop models, solution	10	
Intro computer processing date	1964, Deltamatic reservations system	
DOMINANT INDUSTRIES (fields represented)		
	Marketing Sales, Alliances Partnerships CRS	
ENVIRONMENT		
GOVERNMENT	DOT	
CULTURAL	Non-union	
INDUSTRY	Other airlines, IATA, ATA, ICAO, ACH, ARINC, SITA, ARC, etc.	

Table 65: Summary of environmental factors in *Revenue*

FACTORS	INSTANCE
Public image	State-of-the art software
Belief systems	Computer enhancement is a great benefit to efficiency
Existing practices and routines	New products were simply enhancements to the familiar.
Industry relationships	Ticket processing, travel agents
Regulations	Security, privacy, competition
Imitating the solutions of others	American Airlines set the stage for this kind of work.
Goals	Improve profitability while removing *Y2K* bug
Cost management	Reducing cost of unsold seats

The *Y2K solution* in *Revenue* was examined in light of its context in order to assess its rationality or institutionality as an alternative for solving the *Y2K* problem. Given the conditions of the *Revenue* systems and other requirements, the solution was considered rational. Table 66 shows the factors related to the assessment.

Table 66: Factors related to the response assessment in *Revenue*

OPERATIONAL DEFINITIONS	FACTORS: RELATED TO *Y2K SOLUTION* IN *REVENUE*
Institutional model	(*Y2K* Contingency: *Y2K bug*)
CATEGORIES OF EVIDENCE RELATING TO AN INSTITUTIONAL PROCESS	FACTORS THAT CONTRIBUTED TO AN INSTITUTIONAL PROCESS
Cultural • Related to a social fact: perceptions of air transportation, information technology, information security, safety or other value • Cognitive, e.g., military culture • Familiar, comfortable, habitual, e.g., family culture • Related to established relationships, e.g., vendors	11. Conditions in business area and its IT systems: • Systems working but not as efficient as possible • Employees comfortable in computing environment • Comfortable in dealing with vendors and outside consultants 12. Character of business area environment: • Government agencies challenged in regulatory oversight (DHS, DOJ) 13. Distraction of other business area contingencies: • Financial status • Economic conditions

Table 66 continued

OPERATIONAL DEFINITIONS	FACTORS: RELATED TO *Y2K SOLUTION* IN *REVENUE*
CATEGORIES OF EVIDENCE RELATING TO INSTITUTIONAL DECISION-MAKING	FACTORS RELATING TO INSTITUTIONAL DECISION-MAKING IN RESPONSE TO *Y2K*
Regulatory • Requirements for maintaining organizational legitimacy Mimetic (Following the crowd) • Fashionable, popular • Recommended by vendors • Inadequate information about experiences outside organizational boundaries (reporting only successes)	14. U.S. laws, industry regulations: • Industry regulations were focused on protecting the competitiveness of air transportation, not information privacy and security • U.S. govt agencies' systems not *Y2K* compliant • Industry regulations focused on terrorism threats, passenger screening, but inadequately researched, equipped, and trained. • Industry regulations linked to intelligence gathering—a public concern strongly related to privacy, but not linked to information security 15. Character of business area environment: • External chaos because of time limitation • Mixed understanding of the risk • Scarcity of personnel resources • Good products in the marketplace
Rational-contingency model	
CATEGORIES OF EVIDENCE RELATING TO A RATIONAL PROCESS	FACTORS THAT CONTRIBUTE TO A RATIONAL PROCESS IN IT MANAGEMENT
Goal orientation Actions relating to efficiency and effectiveness Communications related to mission control	7. Organizational leadership: • Acted on the opportunity for improvement, which made the enterprise more competitive • Stayed actively and personally involved in order to insure success. 8. Condition of business area and its IT systems: • Process put in place to assure continual assessment with respect to condition of systems and efficiency of performance 9. Responses to business area contingencies: • Focused on improving possibility for efficient operations.
CATEGORIES OF EVIDENCE RELATING TO RATIONAL DECISION-MAKING	FACTORS RELATING TO RATIONAL DECISION-MAKING IN RESPONSE TO *Y2K*
Regulatory Requirements for maintaining organizational effectiveness Decision-making criteria • Based on knowledge of systems o *Y2K* compliance o Fit with functional area o Efficiency related to cost, processing, resources, etc. o Security	9. U.S. laws, industry regulations: • Bounding framework of concern by govt/industry rules wherein the information in IT systems was recognized as vital to safety and national security, but chaotic wrt policy 10. Organizational leadership: • Knowledgeable about the value of information accuracy and availability • Understood the contribution of IT to the functioning of the organization • Employed personnel with high levels of skills • Adequately responded to security contingencies 8. Character of business area environment: • Personnel resources were adequately aligned with requirements • IT products to serve the needs in *Revenue* were available in the marketplace

The institutional environment was changed dramatically by deregulation. Even though seat prices and routes had been controlled previously, there was already activity in place moving airlines toward competition. When American Airlines began to use its CRS system for data mining, instead of for simply automating reservations, the associated computer programs began to be viewed as tools for seat pricing, therefore better prediction mechanisms for revenue production. Delta and the other major carriers followed suit. Such software was crucial to the airline's profitability and competitiveness; and thus they developed it in-house and did not want to share it with their competitors. The fact that Delta is now able to purchase such seat pricing software commercially is evidence of the institutional evolution in the air transportation environment. The simulation of routing and other flight characteristics is increasingly complex due to the changes in both the technology and in the software development community. Within this institutionalized environment, the *Revenue* business area decision to stay current with the developments with this type of sophisticated software is completely rational. Future revenue and business alliances will be improved with the changes enabled by this *Y2K solution.*

Summary

This chapter traced the history of the Year 2000 Program in four sub-cases over the period from 1997 to 2003. The *Y2K* deadline coupled with considerations associated with financial and economic conditions positioned the implementation of some of the *Y2K solution*s beyond the year 2000 rollover, thus extending the study window from 2000-2003. Each sub-case presented one of the four core business areas in four sections. (1) *Y2K solution*, the compliance decision; (2) *Functional and resource overview*, the

task environment; (3) *Institutional context*, the cultural and regulative aspects of the organization-environment system; and (4) *Response assessment,* the nature of the decision given the contextual conditions. Metrics, which included both organizational statistics and results of Year 2000 Program assessments, were presented in tabular form to enable comparison of contexts across sub-cases. The institutional contexts of individual business areas revealed different organizational cultures and different regulative structures. The cross-case comparisons are presented in Chapter 8.

CHAPTER 8

COMPARING THE SUB-CASES

> Environment as institution assumes that the basic process is reproduction or copying of system-wide (or sector-wide…) social facts on the organizational level … (Zucker, 1987, p. 444).
>
> … the dominant assumptions, language, and ideas of economics can exercise a subtle but powerful influence on behavior, including behavior in organizations, through the formation of beliefs and norms about behavior that affect what people do and how they design institutions and management practices (Ferraro, Pfeffer, & Sutton, 2005, p. 20).
>
> This logic of consequences can be contrasted with a logic of appropriateness by which actions are matched to situations by means of rules … (March, 1994, p. 57).

This dissertation has provided support for the theoretical perspectives of prior works that have demonstrated the power of institutional aspects of environment to influence the actions of organizations. Four business areas were examined as embedded sub-cases of Delta to determine how each responded to the *Y2K* compliance mandate. A final step in the investigation is to compare the sub-cases to determine whether the same relative causes can explain the differences in solutions adopted for dealing with the same problem. Toward that end, the objective of this chapter is to analyze the similarities and differences across the four sub-cases and attempt to isolate causal mechanisms. Discussion focuses on the relationships between sub-system environments and changes in IT systems across the sub-cases.

Summary of sub-case analyses

The results of the sub-case analyses in Chapter 7 have shown that

- In Sub-case 1, *Airport Customer Service*, the *Y2K solution* was rational. It was consistent with the Future Vision goal and the Year 2000 Program goal. Even though it was impossible for Delta to make a completely rational evaluation of alternatives

and consequences under the time constraint (among other reasons), such an evaluation was itself inefficient. The solution decreased the complexity of IT systems and resulted in improvement in the quality and availability of information, increased predictability of IT systems, and business area operations. Further, the solution increased efficiency in systems maintenance, and in business area activities, which provided financial benefit to Delta. The solution improved the bottom line almost immediately.

- In Sub-case 2, *Operations,* more specifically the Tech Ops division, the *Y2K solution* choice was predominantly institutional. SAP modules were installed as part of a move toward ERP functionality, along with other COTS systems that were chosen to reduce the cost of managing parts inventory and documenting repairs. Incomplete information related to complexity led to this mimetic behavior. Institutional monitoring related to safety regulations, coupled with the increasing complexity of aircraft, had led to greater complexity in the software for management. However, the SAP software was developed to serve a different function, and had not been adequately tested in an air transportation environment. Installing a system that was not specifically designed for the detailed services in maintenance and repair operations, and then "hard wiring" it to the finance function created the potential for greater complexity and risk in the short term. This complexity related to the reengineering of MRO processes that was required to accommodate SAP. However, if the Tech Ops overhaul could be accomplished successfully, because of the integration of these applications across the two business areas, there would be a corporate benefit in total. This choice was the likely result of the prominence of SAP in the software market, as well as the confidence and style of Delta's MRO leadership. The decision to install SAP followed the highly successful project management of the Year 2000 Program, which may have contributed to overconfidence. The complexity in the Operations division did not lend itself to rationality as easily as eliminating the *Y2K* bug.
- In Sub-case 3, *Business Support*, the *Y2K solution* was intertwined with *Operations*. In each of the two sub-cases, the notion of ERP was the driver, an ideal of organizational systems where all organizational elements are coordinated. While

elements of institutional decision-making existed in each sub-case, in *Operations* the choice was predominantly institutional, but in *Business Support* the choice was predominantly rational. In *Business Support*, more specifically the finance function, given the goal of modernization, evaluation of alternatives for achieving this goal could be accomplished with a small array of good choices. Among these choices, *Business Support* had the better opportunity to assure a streamlined experience in system installation when compared to *Operations*. The SAP modules decreased complexity of cross-functional interaction, therefore increased efficiency of operation. Having re-engineered the finance processes earlier in the decade in anticipation of a new architecture, *Business Support* had set up a smooth transition to the new application environment. Because the finance function was highly institutionalized, the "best practices" were time tested and predictable. It would be difficult for an organization like *Delta Technology* to re-create the COTS solution via in-house development and find the process cost effective.

- In Sub-case 4, *Revenue*, the *Y2K solution* was rational. In the context of the deregulated air transportation industry and its intense competition, a strong interaction between institutional and rational forces had led to a sophisticated system for calculating seat prices. The *Y2K solution* choices were limited, but within the constraints of resources, the solution choices offered good alternatives. Given the complexity of the simulation system, it would be difficult to reproduce via in-house development and be cost effective. The solution increased the capability for optimization (i.e., increased predictability) of seat pricing on a flight by flight basis, therefore increased efficiency in *Revenue* operations.
- In the sectoral environment of the air transportation industry, the institutional mechanisms and regulative structures benefited rather than constrained Delta's actions. In contrast, the sub-case environments were constraining to the extent that "best practices," or technical resources, not government or other focused sub-system regulations, guided decisions. Products in the IT industry define choice alternatives. Product decisions are often made in the context of contracts with outside agents. These now-institutionalized practices in the IT industry related to commercial developers and "integrators" have led to a structuring mindset of how such exchanges

happen. Historically, no provisions for security have been made or required in commercial contracts. Change in contractual requirements is needed to include an overt sign-off on whether the buyer or seller is taking responsibility for information security. If the buyer of IT services is responsible, the seller needs to verify that the buyer's solution is reasonable and will be implemented. If the seller is responsible, the buyer must have assurance via enforceable penalty.

Cross-case comparisons

This section compares the variable items that were presented in the embedded sub-cases. Table 67 presents a comparison of the *Y2K solution*: *Functional and resource overview*, *Institutional context*, and *Response assessment* across the four sub-cases. Broad similarities and differences among the four sub-cases are displayed in Table 68.

Table 67: Cross-case comparison

	SUB-CASE 1 ***AIRPORT CUSTOMER SERVICE***	SUB-CASE 2 ***OPERATIONS***	SUB-CASE 3 ***BUSINESS SUPPORT***	SUB-CASE 4 ***REVENUE***
Y2K solution	• Fiberoptic networks installed at airports • Kiosks • Large screen displays • Flight-information system • Gate agent / passenger boarding system • Baggage handling system • Standardized desktop units replaced green screens	• Supply-chain system • Supply-chain management • Parts management system • Technical documentation system • Standardized desktop units replaced existing PC systems	• Financial management • Business analytics • Supply-chain management • Standardized desktop units replaced existing PC systems	• Revenue optimization system • Flight network analysis system • Sales automation system • Standardized desktop units replaced existing PC systems
Function	Airport ticket / gate ops	Aircraft operations, flight crew	Finance, HR, legal, purchasing	Marketing, sales
Dominant industries	•Customer relations	•Aircraft maintenance •Aircraft operations •Flight crew •Catering •Corp safety	•Accounting •Auditing •Communications •Facilities mgmt •Finance •HR •Legal •Tax	•Marketing •Sales •Alliances •Partnerships
Industry relationships	Ticket processing and travel agents	Boeing, other suppliers, ATA, IATA, ICAO, hospitality, catering, ACH, ARINC, etc.	ABA, AICPA, FASB, local banks, independent auditors	Other airlines, IATA, ATA, ICAO, ACH, ARINC, SITA, ARC, etc. (Ticket processing, pricing.)
Nature of the work	Routine / dynamic	Unpredictable / complex	Routine	Dynamic
Size No. of PDNs No. of empl	• 47 •	• 248 • 40,000	• 127 • 3,500	• 62 • 10, 000
No. of locations	180 airports plus Atlanta headquarters campus	180 airports plus Atlanta headquarters campus	Atlanta headquarters campus plus finance operations in foreign locations	Atlanta headquarters campus
Date of first computer-based processing	Deltamatic reservations system in 1964	Processing of crew schedules before 1989.		

Table 67 continued

		SUB-CASE 1 *AIRPORT CUSTOMER SERVICE*	SUB-CASE 2 *OPERATIONS*	SUB-CASE 3 *BUSINESS SUPPORT*	SUB-CASE 4 *REVENUE*
No. of systems	1997	119	216	179	102
	2003	129	240	218	122
System criticality H / M / L	1997	36 / 35 / 48	86 / 59 / 71	19 / 53 / 107	24 / 77 / 1
	2003	36 / 34 / 59	105 / 57 / 78	20 / 56 / 142	26 / 84 / 12
LOC (millions)		6	25	12	10
No. of languages		13	31	16	16
Waivered systems		9	46	17	33
COTS systems	1997		32	111	
No. of desktop units		20, 000 (estimate)	3,350	585	529
Desktop models	Orig	53	6	51	13
	Sol	23	3	2	10
% reduction		57	50	96	23
Cultural context		Delta family, "southern hospitality," non-union	Delta family, union (ALPA, PCF-CA), military mentality, "trust arrangements"	Business ethics, strength of the regulatory system, non-union	Computer enhancement a great benefit to efficiency, non-union
Public image		Airport displays and kiosks	Successful installation of SAP is the "envy of the industry"	"The best run companies use SAP"	State-of-the art software
Existing practices		New airport settings and information displays were reformulations of the familiar, for both customer and Delta agent.	Shop workers do not need improved software to perform their jobs well, that's for the "geeks" and "suits." Pilots work best with checklists.	Strongly supported by IT systems, comfortable with standard suites of business applications.	New products were simply enhancements to the familiar.
Government		DHS / TSA, DOJ (Security, privacy, anti-trust)	FAA, OSHA, EPA, NWS, Customs, DOT, etc. (Workplace safety, aircraft / flight safety)	SEC, OSHA, IRS, DOT, DOJ (Tax, HR, accounting, securities)	DOT, DOJ (Security, privacy, competition).

Table 67 continued

	SUB-CASE 1 ***AIRPORT CUSTOMER SERVICE***	SUB-CASE 2 ***OPERATIONS***	SUB-CASE 3 ***BUSINESS SUPPORT***	SUB-CASE 4 ***REVENUE***
Quality of information	Custom systems development and installation by highly skilled in-house employees.	Tech Ops system information based on "best practices" in other industries, other functional areas, but limited with respect to MRO.	SAP systems were proven and developed for the finance function. Environment highly institutionalized and stable.	Systems algorithms were proven and developed for the automated pricing and sales functions.
Predictability	Increased (Improved information, reduced complexity)	Decreased (increased complexity)	Increased (Improved information, reduce complexity of operations)	Increased (Improved information, reduced complexity.)
Efficiency	Increased (reduced cost, potential for increased revenue)	Unknown (potential for reduced cost and increased revenue)	Increased (Improved information, centralized processing)	Increased (reduced cost assoc with unsold seats)
Cost management	Deferred rollout depending on budget	Deferred installation based on resource requirements.	Deferred installation based on resource requirements.	
Mimesis	"Airport of the Future," elements of BNI solution	"The best run companies run SAP."	"Airport of the Future," SAP	American Airlines set the stage for this kind of work. Deregulation and IT created the environment for continuing.
COTS	All hardware and networking equipment	Flight Ops systems developed in-house with a few additional COTS products. COTS crew scheduling, Technical supply chain mgmt, parts inventory and records documentation.	All new software systems were COTS.	All new software systems were COTS.
Best Practices	•Real-time information •Web-based reservations •Call centers •Handheld devices	•OCC real-time monitoring •Tech Ops re-engineering / MRP •Maintenance profit center •Ground Ops devices	•Centralized processing •Finance re-engineering •Outsourcing •MRP / ERP	•Automated pricing models •Sales automation •Alliances & partnerships for marketing & sales
Response assessment	Rational	Institutional	Rational	Rational

Table 68: Highlighted similarities and differences

	SIZE / COMPLEXITY	NATURE OF THE TASKS	*Y2K SOLUTION* DEVELOPED IN-HOUSE	COTS SOLUTION AVAILABLE	MIMESIS / BEST PRACTICE	COMPLEXITY	EFFICIENCY	PREDICTABILITY	RESPONSE ASSESSMENT
SUB-CASE									
AIRPORT CUSTOMER SERVICE		Routine / dynamic	✓		✓	↓	↑	↑	**Rational**
OPERATIONS	Largest, most complex	Complex / dynamic		✘	✓	↑	?	↓	***Institutional***
• Tech Ops		Complex / dynamic		✘	✓				
BUSINESS SUPPORT		Routine		✓	✓	↓	↑	↑	**Rational**
• Finance		Routine		✓	✓				
REVENUE		Dynamic		✓	✓	–	↑	↑	**Rational**
• Revenue accounting		Dynamic		✓	✓				
• Sales		Dynamic		✓	✓				

Discussion of results

> Since Delta had initially planned to use an outside organization to do the Year 2000 Program, they had budgeted $160 million for the project. Delta spent $110 million by doing the work in-house (Taylor, 2004).

The focus of this dissertation was on organizations and their IT systems, and on the interplay between their technical and non-technical aspects. The hypotheses were based on mutually exclusive views of an organization system—alternate conceptions of an organization as either focused on efficiency or legitimacy, and decision-making as either rational or institutional. The criteria for evaluating a *Y2K solution* as rational included: (1) whether or not adequate information was acquired, (2) whether or not a rational choice process was followed, and (3) whether or not evidence revealed solution choices that (a) decreased complexity, and / or (b) increased efficiency and predictability. The criteria for evaluating a *Y2K solution* as institutional included all of the aforementioned criteria, in addition to one or more of the defining institutional mechanisms or processes:

regulative, e.g., environmental agents in institutionalized sectors, in established business relationships, and in State regulatory agencies;

cultural, e.g., social facts extending from the business area's own historical structures and processes, e.g., routines related to historical imprinting, trust arrangements with resource suppliers; and

mimetic, e.g., adopting solutions of other organizations, especially when uncertain about alternatives or under time constraints.

Theoretical inconsistencies

While this dissertation alleged that performing *legitimately* rather than efficiently was the ultimate driver for Delta's solutions, the case study evidence has revealed an amalgamation of rational-contingency and institutional features. Sometimes the organization performed as an institutional system (institutional) model and sometimes the organization performed as a rational-contingency system (rational) model.

In the planning, inventory, and assessment phases, the rational-contingency concept seemed overwhelming. A "best way" was configured at the outset based on a standard project methodology, and the organization adapted to contingencies along the way, principally confronting new learning about the problem, and about the resources available to make the project function efficiently. The formal evidence of rational features included the extensive effort to create planning and documentation structures. Leadership and communication / reporting mechanisms were in place to accomplish the goal according to a phased time schedule.

In the renewal (treatment) phases, the institutional aspects became visible. These observations suggested that a combination of the two contrasting organizational theories presented in this study would offer a more generalizable and comprehensive approach to studies of large complex organizations.

Explanations from rival perspectives

The rival organization theories explain the *Y2K* solutions differently, even though both models consider that organization structure and performance are affected vitally by environmental influences. A rational-contingency system perspective on Delta's *Y2K* solutions considers the *Y2K* compliance plan as a rationalized blueprint for achieving a

predetermined goal. The scope of the Year 2000 program had a clear definition. Tasks associated with eliminating that *Y2K* bug and modernizing the IT systems were organized precisely. The division of labor and marching orders were assigned. Each business area contributed its part to implementing the plan as efficiently as possible in each case. A coordination mechanism provided integration of the parts. According to a rationalist perspective, the differences in business area solutions strictly related to the diverse activities that each business area performed and the kinds of technical equipment required for supporting those activities. Any deviations from the goals were caused by technical environments and resource limitations. The evidence from the Delta study that the organization performed according to a rational system model included features such as:

1. organization of four business area teams, including the division of labor and coordination mechanisms that enabled Program integration and control
2. focus on the goal of eliminating the uncertainty associated with the *Y2K* vulnerability, and uncertainties associated with complexity
3. complete information to achieve the goal
4. decision-making of the business area teams based on efficiency criteria

Like this dissertation, studies employing rational system models (e.g., Lawrence & Lorsch, Woodward), which were described in the section on contingency theory, have shown that organizational differentiation is related to resources and requirements of the sub-unit's particular task environment. These studies explained sub-unit actions by observing that they faced relatively unique environmental demands related to their associated sub-environments, and described a process of adaptation that leads to *variation* in structures and practices among different kinds of organizations as they pursue their goals. However, different from this dissertation, conclusions were based solely on the perspective of a rational-contingency model. Rationalists argue that organizational sub-units have freedom to choose their actions within the scope of their functional

subsystems, and they do so based on economic principles. This dissertation does not show evidence entirely in conflict with this notion, but augments these ideas to include the influence of institutional contexts.

In contrast to the rational system model, an institutional system model portrays the business area *Y2K* solutions—and the development of the Delta Year 2000 Program—as a contextualized process shaped by institutional mechanisms. These institutional mechanisms include such constructs as historical values, perceptions, and judgments. Such mechanisms contribute to more explicit channeling provided by regulative mechanisms, such as marketplace supplies of COTS products, consultants and vendors, technical resources, and other forces in the organization's wider environment.

Consistent with an institutional system perspective, data from this Delta study revealed that business areas in part acted to satisfy values. These included, but were not limited to a familiarity and consistency of the presentation of the Delta image to the public, its employees, and the larger air transportation community, as well as a desire for more modern equipment and greater management control provided by improved information. In addition, business areas may have made certain decisions simply because the resources were available to do it. In fact, one informant said they had so much money to spend on the project, they had no opportunity to spend it all in the short time frame prior to the Year 2000 rollover.

The Delta solutions far exceeded the goal of eliminating the *Y2K* bug, and some solution elements may have served no verifiable contribution to efficiency or effectiveness if the ultimate costs and benefits were weighed. Ideas of efficiency in some cases were secondary to the larger attempt to position Delta as a more competitive, and

legitimate player in the fast moving air transportation environment. If that had been the case in total, differences across business areas would have had their origins solely in the histories of the business areas, and, more specifically, in the histories of the fields—i.e., wider sectoral environments—represented by the respective business areas.

Evidence that Delta performed according to an institutional system model included features such as:

1. a focus on multiple goals, some of which transcended eliminating the uncertainty associated with the *Y2K* vulnerability
2. inadequate information to support decisions
3. decision-making of the business area team based on routines and familiarity, and other legitimacy criteria
4. modeling solutions of other organizations in their industry sector
5. implementation of solutions based on industry "best practices," without ways of evaluating their efficacy in specific circumstances

Airline-related organizations constitute an organizational field; therefore, institutional theory predicts that over time, a process of isomorphism produces similarities among these organizations. However, the industries and professions associated with individual organization business areas also constitute organizational fields: the accounting industry, airline operations, the marketing industry, the information technologies industry, etc. Employing an institutional system perspective, this study has demonstrated how business area interactions within their respective institutionalized sub-environments shape airline development and functioning.

The institutional system idea of this dissertation placed the rational model in a context of institutional processes that were shared with others in particular fields. Following the logic of Lawrence and Lorsch, it was reasonable to assume that relatively unique sub-environments may have included institutional as well as technical aspects and that fact has been confirmed. Similarities in the structures and practices of organizations

in the same field are the visible display of conformity to what is understood to be legitimate in their respective contexts, and not necessarily targeted toward achieving organizational purposes with greatest efficiency—especially under conditions of uncertainty.[133]

> … [H]ighly structured organizational fields provide a context in which individual efforts to deal rationally with uncertainty and constraint often lead, in the aggregate, to homogeneity in structure, culture, and output (DiMaggio & Powell, 1983, p. 147).
>
> The more uncertain the relationship between means and ends, the greater the extent to which an organization will model itself after organizations it perceives as successful (Ibid., p. 154).

Under conditions of uncertainty, network ties across organizational boundaries are especially influential with respect to choice of organization to imitate (Galaskiewicz & Wasserman, 1989). Evidence indicated that there was uncertainty regarding means for Delta's *Y2K* compliance. In response to this, Delta's Board of Directors recommended locating a consultant to assist in designing the Year 2000 Program. The choice of The Feld Company, one of many consulting organizations involved in the process, came from Grinstein who had witnessed a successful IT project at another transportation organization. Delta has been given credit for being innovative as an airline company with regard to its information systems strategies, but similar experiences in other organizations, esp. from within the transportation sector, led Delta to adopt such strategies. However, the impetus for using the strategies came from Delta's Board (Greising, 1997).

Each of the *Delta Technology* application portfolios reflected the activities of a functional division of Delta Air Lines. Among all of these cooperative teams, each

---

[133] It is important to note that organizational systems must serve many values and purposes, not only efficiency.

respectively represented an unrelated field and therefore was included in a somewhat distinct sub-environment. Sub-environments differ in their propensity toward institutionalization depending on their respective histories and cultures. This dissertation has demonstrated that isomorphism, the process by which standards of legitimacy are diffused within organizational sub-environments, can account for variation in the *Y2K solution* of the business areas at Delta, wherein most of the *Y2K* solutions were the result of a rational choice process. The "standard of legitimacy" related to the concept of an industry best practice, a rational / institutional concept.

Multiple levels of context

Each *Y2K solution* was the result of activities that took place in a business area over five to six years within a number of contextual levels. The levels of context included the air transportation sector, the Delta and *Delta Technology* organizations, the Year 2000 Program, and the respective environments of each business area.

In all four sub-cases, the environments were the same with respect to the air transportation sector and the enterprise organizations, i.e., Delta and *Delta Technology*. With regard to the enterprise contexts, in 1997 *Delta Technology* had been so recently established that many institutionalized elements of the Delta and *Delta Technology* contexts were the same. Further, in the four sub-cases, the same methodological framework defined the assessment and remediation process of the Year 2000 Program. The sub-case comparison therefore controlled for all of these higher level environments

to the extent that the business area solutions could be related to the context provided by their respective sub-system environments.[134]

All four business areas made decisions to remediate code and to replace hardware and software. All four installed desktop units with as much standardization as possible. However, other solution elements were different. These different elements thus related to the distinctive contextual conditions in each of the areas.

Comparing task environments

The *task environment* comparison shows that *Operations* was the largest business area in numbers of employees and numbers of divisions. *Operations* had the greatest amount of complexity in its activities, which was reflected in the number of divisions, and in the numbers and complexity of its systems. The systems in *Operations* had a greater total number of LOCs, written in more programming languages, than the systems in any of the other three business areas.

The Desktop Strategy Project was a comprehensive evaluation of all desktop units and their system configurations enterprise-wide. The results of the inventory and assessments performed for this project provided another measure of the complexity of the task environment in a business area. *Airport Customer Service* had a greater number of desktop units, and showed the greatest amount of complexity among the desktop unit models. While the complexity was reduced in all four business areas because of this project, *Business Support* showed the greatest percentage reduction in the number of desktop models. *Airport Customer Service* was next, followed by *Operations* and *Revenue.*

---

[134] Note that the "system" referred to here is the organization and its sectoral environment.

Comparing institutional environments and response assessments

Along with the differences in task environments, differences in perspective existed throughout the Delta organization. Cultural and cognitive divisions were extreme—the unionized pilots and "everyone else," the military (therefore, rational / strategic mentality) and family (cultural persistence, therefore, institutional mentality); the institutionalization of the concept of safety and a disconnection with the concept of information security. In this dissertation, these differences related to the concept of complexity in a business area.

Wider environments

In addition to the task environments and institutional environments internal to Delta, competitive market conditions and the time deadline of *Y2K* affected solutions. Competitive market conditions, in terms of available COTS solutions and existing best practices, appeared to be the important preconditions to sub-organizations seeking the assistance of vendors and consultants in lieu of developing systems in-house. Vendors and consultants thus provided a principal mechanism for institutional influence. In all four business areas, however, there was conspicuous evidence of rational decision-making related to improvement in performance efficiencies.

The prominence of the *Y2K* event and its associated deadline had a strong influence on the Year 2000 Program in total. *Y2K* improved the focus of executive management and improved the efficiency of project management. Without the deadline and urgency to make changes to the IT systems, Delta might have continued to operate its information systems in a mode of responding to needs for development and repairs according to which system had crashed or become inadequate for producing a particular

output. Consideration for the economic benefits to be gained by completely transforming the IT systems might have been deferred for a long time. Additionally, the information security vulnerabilities that were inherent in aging systems, especially those with high levels of complexity, might have eventually led to disastrous consequences.

The evidence provided by the creation of the OCC (*Operations*) and the CustomerCare system (*Airport Customer Service*) showed that the capability—the ideas and skills—were present to develop the increased functional efficiency in-house via state-of-the art systems. However, the OCC was an ad hoc addition, a one-time notion in an isolated division and an earlier response. Similarly, the CustomerCare system in the *Airport Customer Service* business area had been in the works prior to the Year 2000 Program launch. Before the crisis of *Y2K*, the justification had been missing that would have brought about the planning, synchronizing, and maintaining of systems enterprise-wide in order to achieve maximum economic benefit—even though envisioned by IT experts for years.

The *Y2K* time deadline, important to the Year 2000 Program in total, had minimal effect on a *Y2K solution* in an individual business area. The timing of installations was affected in some instances, but in most areas, not the solution itself. The criticality assignments during the systems assessment phase gave priority to high critical systems, so that code remediation and other actions were performed on these systems first. Certain systems were evaluated as needing replacement, and if the replacement was a complex implementation, the complete solution was delayed until after the year 2000 rollover. All of the business areas deferred at least a part of their solution activities until after the rollover. The fact that all of the business areas were successful, with a few minor

exceptions, in meeting the *Y2K* deadline without incident rules out the time deadline as an influence that differentiates the sub-case decisions.

However, the focus and funding of *Y2K* may have set up the institutional decision-making that was evident in the Tech Ops solution. The development of the DNS, and the ideas associated with modernization were strongly influential to the Tech Ops solution. Further, all of the solution choices were made from within a narrow view and resulted in unanticipated information security impacts.

Transformation: not a radical leap

The puzzle that existed at the outset of the study—at Delta's agreement to a "transformation" while eliminating the *Y2K* bug—diminished significantly with the knowledge gained through this investigation. The transformation, while still a "bold move" for Delta, was not a radical leap forward into a new IT environment with which the organization was completely unfamiliar. The organizational changes at first seemed to be adding complexity, but lessened in dramatic appearance upon further analysis.

Organizational restructuring

The "cultural revolution" reported by one of the informants had seemed inefficient. In actuality, the organizational restructuring enabled greater efficiency in achieving the changes that had been designed by the CIO. The placement of highly skilled employees or consultants in *Y2K* leadership positions enabled faster accommodation for the major changes in the infrastructure environment. This leadership was extremely important given the time constraint and the limited visibility of the teams. The leadership was clearly lacking, however, in terms of planning for the consequences to information security.

Institutionalism and rational decision-making: What *could* they be thinking?

The cross-organizational make-up of the Year 2000 Program teams, with each team confined to a business area, reinforced a restricted "business area view" of the world.

> We all have a tendency to some degree to run on a mental "autopilot" - whether you want to call this phenomena "framing," worldview, paradigms, schemas, ideological constructs, etc. - the precise meaning vary [sic] but the effect is to shape our perceptions of the world (highlighting or omitting data) and to an extent predetermine our responses in a large picture sense. Ideological blinders concentrates [sic] our vision but they distort our view of reality (Safranski, 2005).

The compartmentalization and narrow focus of the bureaucratic structure decreased the rationality of the choice process in a business area, limiting consideration of all the consequences of their decision alternatives. To these blinders add additional sets—the narrow focus of the business area IT systems themselves, and the associated work environments, and the image becomes that of a team of workhorses.

Each member of the team is shackled to the other and each must drag behind some share of the workload, the workload being a specific segment of systems dedicated to specific business area activities. However, each in the team is wearing his / her own set of blinders. Therefore, the one cracking the whip must know the destination and the best way to get there, because the workhorses are unlikely to speak up. They have worked in this configuration too long to expect or even think about change.

There were four of these "workhorse teams" operating in their own respective spaces at Delta. Note that one of the main complaints about the architecture of Delta's systems prior to the transformation was that they operated in "information silos," without enough cross communication to enable information to be available, accessible, and accurate for all functional purposes. There had been "18 little disconnected fiefdoms"

(W. Taylor, 2004). Was the business area structure of the Year 2000 team, therefore, the "best way" to develop new solutions? It formed yet another institutional context within which the "rational" solution designs were produced.

Changes to IT were incremental

The results of the Delta transformation seemed dramatic to an outside observer because the reliability of information and its visibility had taken such prominence. Further investigation led to the understanding that Delta had been gradually augmenting its systems' capabilities across the business areas over the years.

The most striking major additions brought about by the transformation were to the reservations systems. These systems had been in use since the 1960s and improved throughout the 1980s. However, when the Internet and the DNS enabled online reservations systems in the 1990s, the world of CRS systems of the past was transformed completely.

Similarly, improvements had been made gradually to the finance systems over time. Then in the early 1990s, major re-engineering of processes and systems was accomplished; the project ran six years from 1990-1996. This streamlining of the finance function was strongly connected to the influence of the regulative environment. The similarity in the finance function across all industry sectors had led to faster evolution in software support. The IT marketplace had the best products to serve this functional area compared to the others because of the size of the market, and the routinized processes that had evolved accordingly. The market was directly aligned with the regulative environment. The subsequent changes brought about by DNS during the Year 2000

Program simply enabled a “re-connection” from prior LAN-based systems to those designed with Internet protocols.

The software in the maintenance area had been the latest additions to the parade of automated functions at Delta. Because of its complexity and specialized features that were different from other industries, it was not well-served by commercial software. Paper processes had been automated when the TOPS and MARC systems were installed in the early 1990s, which required process re-engineering. When the new SAP systems were installed, re-engineering was required again, not only because of the DNS connection, but because the software itself had not been designed for such application.

The *Revenue* choice was based on the highly competitive airline industry and its increasing requirement for accuracy in pricing and forecasting because of the changes in IT systems. When the industry was deregulated, each airline was forced into a position of evaluating how to become better than the competition in seat pricing.

The call centers in *Airport Customer Service* area were part of the *Y2K* solution, but not investigated in this study. This mechanism for customer service had become popular, a mimetic solution that is IT related. Most likely in the short term, the solution has been problematic and therefore may be evaluated as institutional. In this case, copying others’ ideas may lead down the road to a mess. The idea was to reduce head count and turn a headache over to outside entities. This move, solely focused on cost reduction, has undoubtedly diminished customer service and created more issues than Delta management ever imagined. The lesson here: do not assume that making changes based on cost alone is a rational act.

Summary

This chapter presented cross-case analysis of the four sub-cases and a discussion of the results. Results showed that performing efficiently was the ultimate driver for each of the Delta business area solutions, even though performing *legitimately* could also be attached to the context of all four. All three of the defining institutional processes were at work in the Delta settings: *regulative*—by external sources, i.e., environmental agents in institutionalized sectors, such as in the professions, in established business relationships, and state regulatory agencies); *cultural*—transmitting social facts from the Delta business area's own historical processes, such as trust arrangements with resource suppliers; and *mimetic*—adopting other organizations' successful elements, especially when uncertain about alternatives. In total, however, within the confines of the study period, the choices were rational within a public regulative system where incentives were aligned. However, with respect to information security, much work was left to be done in the wake of the IT transformation.

CHAPTER 9

WHAT HAPPENED TO INFORMATION SECURITY?

> The recent Year 2000 computer problem is the most remarkable example of global human cooperation I have ever witnessed (Beach, 2000).[135]
>
> Our goal was to operate normally, safely—our regular daily expectation. We achieved our goal and delivered significant computer improvements to the company at the same time (Taylor, 2000, quoted in Delta archive, *Y2K*-Normal.doc).
>
> After Year 2000, there were errors but none were [sic] catastrophic (Taylor, 2004).
>
> By any measure, 2000 was the "year of the virus" for Delta and *Delta Technology*. Employees spent more 24-hour shifts fighting viruses during the year than they care to remember (Davis, 2001, p. 11).

The objective of this chapter is to present the results and experiences of the Year 2000 Program in the context of information security. Recall that Delta's plan focused on a primary and a secondary goal. The primary goal was to eliminate the *Y2K* bug; and the secondary goal was to transform and to modernize the IT systems architecture throughout the enterprise.

Toward the goal of eliminating the *Y2K* bug, the organization operated most of its systems successfully following rollover. Given the complexity of the project, the Delta organization could be enormously pleased with this outcome. The project methodology that the company had purchased had obviously worked for them to assist in locating and repairing most all of the instances of the *Y2K* bug. This methodology was a COTS solution that was available in the marketplace, likely one of many that were available at the time. The methodology had spelled out each phase and each component in meticulous

---

[135] From the prepared testimony of Gary Beach, publisher of *CIO* Magazine before the House Science Committee Subcommittee on Technology and the House Government Reform Committee Subcommittee on Government Management, Information and Technology.

detail. Maybe the nature of this plan distracted employees from a focus on the nature of the problem: the risk that the *Y2K* bug posed for information security. This plan may also have created blinders to consideration for all of the consequences of the solutions.

It is difficult to remember how widespread public awareness was regarding information security in the years leading up to the year 2000, but it appeared that information security was not an overt focus for the Year 2000 Program. However, it is puzzling that the subsequent virus attacks on Delta's computers after year 2000 were unexpected, following such a comprehensive overhaul as the IT transformation. At one point that year, a particularly malicious Outlook bug known as "funlove" had run rampant around Delta's systems without any human intervention. Before it was stopped, the malware had infected more than 200 servers and "countless PCs" (Davis, 2001, p. 11). Another, known as the "love bug," brought down Delta's entire email system. "Nearly 50 DT employees worked around the clock, some for as long as 36 hours at a stretch, to get rid of the problem" (Davis, 2000, p. 12).

Right on the heels of celebrating *Y2K* success, and the renewal of so many aspects of the Delta IT operations, came a new project, "Antivirus Renewal." By the end of 2001, *Delta Technology* engineers had installed new antivirus software on each desktop unit, and integrated the software with server software that would provide automatic updates. Why was this risk not anticipated and the defenses planned and implemented in advance? Before discussing this puzzling situation at Delta, the next section presents other post-2000 events.

Post-2000 incidents and other stories

The enormous efforts of a great many organizations during the latter part of the 1990s paid off in eliminating most all critical issues that were related to the *Y2K* bug. The work was done so well that the *lack* of problems merely underscored for skeptics that the hoopla and expense had been a hoax. Many still believe that all the geeks had collaborated in a great worldwide conspiracy to generate work, and to raise salaries. The truth is that no organization before or after the event wanted to discuss *Y2K*, whether confirming or denying the allegation. Organizations were disinclined to discuss security issues of any sort, even those related to success. However, in spite of all the focus on the crisis and all of the hard work of organizations to remediate their systems, some failed to operate:

- Nine nuclear power plant incidents occurred in Japan, and seven occurred in the U. S., all of which were attributed to minor electric power supply problems. According to press reports, the incidents did not involve a compromise of safety-related systems or require plants to be shut down. (The Daily Yomiuri, Tokyo, 2000, Jan 6 and The Los Angeles Times, 2000, Jan 2).
- Point of sale credit card companies posted transactions multiple times to credit card accounts, because they did not download a patch (Computerworld, 2000, Jan 17).
- The U.S. Defense Department experienced computer failures related to processing imagery from intelligence satellites, which resulted in an interruption in the flow of spy satellite information. The Pentagon insists the trouble did not jeopardize U.S. national security (The Associated Press, 2000, Jan 14).
- Heathrow airport lights malfunctioned. A Delta informant said they could not be helpful with the problem, since Heathrow systems were completely different from anything Delta had installed at Hartsfield.

A number of high profile interruptions to critical infrastructures have demonstrated the chaos that such incidents can create. As mentioned in Chapter 1, the blackout in the Northeast and Midwest part of the U.S. in August 2003 is an example. Many companies use diesel generators to keep backup systems running, but as the

gigantic power outage demonstrated, the diesel can run out if the backup systems are in continuous use. In such cases, companies must take special steps. Following the 2003 blackout, Delta arranged for generator fuel to arrive by helicopter in the event of another shortage. (Nolan & McFarlan, 2005). However, as this example illustrates, the correction is often made after the damage is done. Further, and possibly more problematic, is planning a solution without adequate information, as the next example illustrates.

Presenting the solution before considering all consequences

Proponents of a new flight-tracking technology are pressing to have ADS-B transponders mandatory equipment on all aircraft so that all aircraft can be accounted for in U.S. airspace (Doyle & Gillies, 2007). However, this technology puts crew and passengers at risk. A pilot has described how easy it would be to intercept the signal from this particular type of transponder and use it to bring down an aircraft (Philips, 2000). Is this a hasty solution that is the result of exposing limitations in the FAA's flight tracking in the details of the JFK Jr. crash?

This is what happened. The plane went down around 9 PM on a Friday and the search and rescue efforts began at 6 AM Saturday. Those efforts continued, under intense press scrutiny, through all of Saturday, all of Sunday, and all of Monday. Around midday Tuesday, the FAA finally decoded enough of their radar tapes to determine where the plane went into the water. At that point, the remains of the aircraft were found quickly. The FAA had spent more than 72 hours trying to locate the aircraft, an aircraft that the President of the United States and the world press corps were actively interested in finding. It was evident from the experience that the FAA did not possess the resources to track the volume of flights for which the agency was responsible. Does the promotion of

mandatory ADS-B transponders suggest that policy-makers are rushing into a solution that will create more problems than now exist? Could we propose that this was the same situation when Congress approved the change to the scheduled daylight savings time for 2007?

Information security at Delta after the Year 2000 Program

> The system is not finished. In the works are more customer-facing applications, operations and revenue management functions and—a new need—security (Robb, quoted in "Technology Leadership: Delta Technology," 2004).
>
> Sarbanes-Oxley (Sarb-Ox) pressures require reconciliation of systems to tie back to general ledger. Just because you reconcile doesn't mean you pass. How you manage your systems and controls could lead to a material variance. Sarb-Ox is interested in behavior as well as systems security aspects. It is not clear exactly what Sarb-Ox requires; auditing is interpreting the meaning. Operating areas are the central aspects of compliance, well beyond the financial aspects (Taylor, 2004).
>
> Delta Air Lines Inc. and AMR Corp's American Airlines Inc. also confirmed that the stolen computer contained some of their customer data (Rosencrance, 2004).

Because of the technology improvements that resulted from the Year 2000 Program, real-time financial information was available to executives, which especially benefited them as they have managed through Delta's difficult financial circumstances. However, in light of the development of the new threats to IT security that were developing in the late 1990's because of wider network access, it is surprising that concerns for the security of this information were not more conspicuous in the Year 2000 Program plans. A role that was defined as part of the BDM methodology was that of Risk Manager:

> Risk Manager - establishes a risk plan concerned with identifying, analyzing, mitigating, monitoring, & controlling risks in the Year 2000 program for business/functional, costs, schedule, technical/operational (Delta archive, Sec 1).

This title would suggest that a process was in place to account for the technical security of the new systems. However, when asked about security strategies, informants have

seemed to go blank. In fact, it was unclear that plans included data protection for the systems beyond code remediation or replacement to rid them of the *Y2K* bug. Information security was rarely mentioned in the Year 2000 Program documentation. Later, *Delta Technology* CEO Robb (when interviewed in 2004 about the remarkable successes of *Delta Technology*) was quoted as saying the next problem that the organization needed to address was security ("Technology Leadership: Delta Technology," 2004).[136] That is because the standardization, network connections, and other changes that led to the efficiency improvements had also generated disruption to "business as usual" for the IT users and actually created other security problems where none had existed before.

Delta's flight attendant scheduling system

Following the year 2000 rollover, "a flight attendant scheduling system malfunctioned, along with around 40 other non-critical systems" (Taylor, 2004). However, no one at Delta is inclined to talk about these kinds of incidents.

> Delta Air Lines Inc. declined to comment about the cause of a systems glitch that forced it to cancel about 40 flights and delay an unspecified number of departures on May 1. The Atlanta-based airline has "resolved the situation," said a spokeswoman. But, she added, "as a matter of company policy, we will not provide additional information on the issue to ensure the protection of our IT systems" ("Delta stays mum on cause of IT glitch," 2004).

Clearly, systems are more vulnerable when they are all tied together and connected to a common information repository. This is the familiar tradeoff between efficiency and security. Web-based applications that add efficiency to the development and maintenance process also create information security issues that require careful

136 Robb joined Delta Technology in late 1999 as CTO, and became Delta's CIO in 2000.

management practices. However, historically vendors and consultants have not been concerned with the security of the clients' or their clients' customers' information.

> [SAP] … continues to shift its customers to its mySAP products, which are Web-based software platforms used for a variety of enterprise functions (Hoover's, 2007).

> Between April 2003 and June of … [2004], Delta made a major investment in web-based delivery of technical manuals via the company's intranet site. The new system, known as Flightline, supplied by InfoTrust … hosts 70 maintenance manuals and illustrated parts catalogs covering all aircraft and engines in Delta's fleet. Preliminary planning to make the manuals available on hand-held devices via wireless transmission now is going forward, and will be presented to Delta's management in 2005 for approval.

Wireless devices add yet another set of information security issues. A test for intrusion possibility was conducted at both the Denver and DFW airports around the deadline for mandated baggage systems. The "red team" found that breaching the security of systems for connecting passengers to their baggage was extremely easy.

Comair

In 1997, Comair was a "Delta Connection" carrier, one of the regional airline affiliations that provided extended service to Delta customers. Events connected with Comair show examples of the complex dependency environment in commercial air transportation enterprises.

> The January 1997 crash of Cincinnati-to-Detroit Comair Flight 3272 represented a failure of the Federal Aviation Administration (FAA) to set adequate safety standards for icy conditions, the National Transportation Safety Board (NTSB) concluded Thursday. The NTSB said that "the probable cause of the accident was the FAA's failure to establish adequate certification standards for flights in icing conditions." (Barton, 1998).

An interesting incident regarding Delta's institutional mindset is illustrated by the Comair IT systems "crash" on Christmas Day in 2004, long past the worrisome focus on *Y2K* and other systems vulnerabilities. An ice storm that day required rescheduling a larger number of passengers than the system had processed prior to the crash. When the computer systems exceeded their processing capacity, they simply stopped. As a result,

Comair grounded around 1100 flights and shut down for four days, which cost about $20 million in revenue (Wagner, 2004).

> Comair knew there was a chance there would be a problem. They said they had planned on updating their computer system, but other cost pressures—such as meeting payroll—were too great. So they just hoped that their system, patched together, would work. It didn't. Now they're playing catch-up. (Kasarda, cited in Rothfeder, 2005).[137]

Delta bought Comair (which had been a regional subsidiary) in 2000 then proceeded to resist opportunities to invest in its systems, based on the institutionalized notion that low cost airline means not only low cost for the customer, but low cost for the company.

Another incident involving Comair came in 2006. The Comair jet crash that killed 49 people, some might call a "normal accident." However, it reflects a violation of one of the basic elements of information security: information integrity. On August 27, 2006, a Comair flight filled with passengers bound for Atlanta crashed on takeoff from a Kentucky airport. With the exception of the co-pilot, all of the passengers and crew were killed instantly. Months before the crash, air traffic controllers at the Lexington airport wrote to federal officials complaining about a hostile working environment in the tower and short-staffing on the overnight shift, according to letters obtained by The Associated Press. However, the short-staffing was not the cause of the problem. A Comair spokesperson said the airline was using an airport map with outdated information at the time of the crash.

The positive impacts of Delta's *Y2K solutions*

> In the process of addressing the *Y2K* crisis, Delta invested $1 billion in its IT infrastructure and developed a publish-and-subscribe environment to support a cross-functional customer-orientation (Ross, 2001).

---

[137] Kasarda is a management professor who specializes in airlines at the University of North Carolina.

Delta's overarching objective during the Year 2000 Program was to position its *Delta Technology* subsidiary to be more competitive in the year 2000 and after. The leadership for achieving this goal was extremely important—as was the elimination of the *Y2K* vulnerability. However, information security, as the organization understood it, was not a focus.[138] This goal was a secondary aspect (the *Y2K* bug was the number one priority), that both strengthened and weakened information security. Strength would come by standardizing hardware, replacing outdated systems, and by gaining a better general understanding of how the systems worked. The negative effect would come by standardizing systems and employing a common network protocol to connect them all. However, not all of the effects on information security were negative. A number of positive results offered opportunities for a higher level of security in information systems management.

One of the outcomes was a new position, called Chief Information Security and Privacy Officer.

> Spark Nowak works for Chris Duncan, Chief Risk Officer for Delta. Chief InfoSec Officer, Spark Nowak, is a person whose objective is to oversee policies company-wide, impacting technology through policy. Attack/penetration tests are run out of Nowak's office. Each business unit also has a security officer (BISO), responsible for implementing policies on a business unit basis (Robb, 2004).

Architecture

The institutionalization of standards and practices mentioned above advanced as well as hinder the possibility for optimizing the activities of the organization and thus the supporting information systems. Advancement came with the renewal projects where a multitude of legacy systems and equipment was replaced in airports and headquarters

---

138 An information security department was not established at Delta until 2003.

campus offices. The airport and campus renewal projects replaced dumb terminals with new interactive systems, and provided gate-area information displays (GIDs) that allowed better communication with passengers. Integrating and undergirding all of this was a new infrastructure system that enabled communication among previously isolated systems, and which was designed to make future maintenance easy. These older systems could have been crash-prone technologies, similar to the ones in the Comair incident. In the inventory and desktop system project, the Delta teams had identified over 3,000 unique vendor software and hardware products. To standardize what had been a plethora of platforms and software systems enabled better management of application software.

Business continuity planning

Business Continuity Planning had been an integral part of the Year 2000 Program at Delta, which is a prominent feature of military culture. Mullin gave credit to the *Y2K* planning in enabling better preparedness for 9/11. This was what he said.

> At Delta, we had just started our weekly executive review of company events when the first aircraft crashed into the World Trade Center. Recognizing pretty quickly that this was almost certainly not an accident, we moved the already assembled executive group to Delta's Operations Control Center,—a sort of Mission Control setting—where we watched the terrible events unfold across giant TV screens.
>
> Following the second crash and the FAA's decision to ground all aircraft, we began a task unprecedented in the history of aviation. We used as our blueprint a plan we had formulated to serve as a failsafe in the event of any Y2K issues. According to that plan, each Delta aircraft was instructed, based on their position, to return to the point of origin, proceed to their destination, or find the nearest suitable airport and land immediately.
>
> Within an hour, all domestic flights were on the ground. Forty minutes later, passengers and crew had been accounted for. Landing our international fleet took longer—around three hours—since many flights were over the Atlantic Ocean when they received instructions (2001).

Another positive result following 9/11 where business continuity planning was given credit is an incident with the Delta website. The delta.com website had been

receiving about 70,000 hits a day in 2001. The week of the attack, it saw 10 times that many queries each day. About 130,000 passengers viewed their flight itineraries online that week, compared with about 50,000 in a normal week. Because of its redundant systems in two Atlanta locations, the increased traffic created no problems.

Release management and virtual testing facility

Because of *Y2K*, Delta has an official "release management group," which had not existed before. Prior to *Y2K,* Delta computer specialists had neither constructed nor worked with a testing environment. The testing environment that was created for *Y2K* improved significantly the development and maintenance methodology that ultimately contributed to better information security management. The virtual test facility allowed systems to be tested before returning them to a production environment. They installed a duplicate set of hardware to that of the production environment in order to test the systems. This MVS, C/S, & VM test environment was the first of its kind at Delta. By pretesting, they could determine if the *Y2K* bug had been cleaned and figure out where the software might fail. They could then provide a certified and tested copy of the upgraded software to its production environment.

Asset management

> Data gathered during the inventory estimate will ultimately be used to populate a *life-cycle I/T Asset Management System* for Delta Air Lines. The planned availability date for this system is June 1998, with the expectation that it will be fully populated by December, 1998 (Delta archive, "Year 2000 Hardware Assessment, Impact Analysis and Renovation Project Plan Version 1.0," 1998, p.4).

Managing the risks of IT systems involves decision-making on a regular basis regarding upgrading or replacing IT assets. Delta has a huge bandwidth network worldwide, which requires ongoing replacement of old switches, and other components

related to the operation of mainframes, servers, desktop units, and their voice and data networks. The company has assigned an annual capital budget of $200 million for renewal of this infrastructure. To analyze the relative costs and risks of components, Delta developed a framework that allows for maintenance while staying within this budget (Anthes, 2004). *Delta Technology*'s management developed a weighted score for each combination of business area and IT asset, based on five factors: technology age, business value at risk, platform supportability, platform complexity, and risk of failure. Each would be assigned one of three colored flags, depending on the IT asset in that business area offered a low, medium, or high risk to the airline. The results might show, for example, that the server infrastructure presented a medium risk for *Airport Customer Service*, a low risk for *Operations*, and a high risk for *Business Support*. Table 69 shows the risk matrix they have used.[139]

Table 69: Risk assessment model

	NETWORK	SERVERS	DEVICES
AIRPORT CUSTOMER SERVICE			
OPERATIONS			
BUSINESS SUPPORT			
REVENUE			

Source: Anthes (2004).

Plans for the future

Future planning initiatives for Delta have included converting the Year 2000 compliance database to an asset tracking type database (including quantities and location), and investigating means for expanding the types of data tracked through the

[139] Adding the risk scores in the columns produces a scorecard like this, color-coded for high, medium, and low risk.

database (e.g., tracking which applications actually run on which servers) (Delta archive, COTS state of the union.doc).

And, the beat goes on …

> Delta Air Lines Inc. this week is launching a three-year project to replace its core IT backbone with a service-oriented architecture (SOA). Delta Technology Inc., the IT arm of the Atlanta-based airline, this week will begin the process of updating the Delta Nervous System, an IT backbone used to route messages among multiple systems. The DNS manages everything from tracking passenger check-ins and boarding to the SkyMiles frequent-flier program, the company said. The goal of the project — dubbed DNS 2.0 — is to replace proprietary Tuxedo middleware from BEA Systems Inc., which now runs DNS, with standards-based SOA technology … (Havenstein, 2006).

Summary

The Delta computing environment had changed dramatically because of the Year 2000 Program. While system failures happened following the rollover, they were mostly non-critical systems. However, the consequences to information security were mixed. The web-based applications and standard operating systems in the desktop units created new vulnerabilities. The equipment and methodologies that were put in place to test and manage the Year 2000 remediation process improved Delta's capabilities to manage information security.

CHAPTER 10

CONCLUDING COMMENTS

> [Delta] would never have achieved what we did without *Y2K*. And, 9/11 still has great impact. Delta was very involved at the time and it still strongly affects us. We instantly changed from a $16B to a $13B company. If it happens again, we can't survive (Mullin, 2004).
>
> It is also important to recognize that science is just one of many ways of understanding a world in which changes are increasingly a consequence of human beliefs and behavior. The capacity to respond to complex problems rests on an understanding of this changing context, without which scientific explanations and technical solutions are likely to be irrelevant no matter how precise ("Who We Are," 2004).
>
> The flight operations system, invented from scratch from the space program, proved itself a model of how to make life-and-death decisions in seconds. The proof of the technical excellence of Apollo is its record (Murray & Cox, 2004a, p. vii).

Some might say that a comparison of the rescue of the Apollo 13 flight with that of the Mission: Year 2000 Program is an apples and oranges comparison. The computer technologies involved in the two emergencies were light years apart. In the Apollo system, "all three stages of the [rocket] booster plus the command module and the lunar module—had less computing capacity combined than today's typical cell phone" (Ibid). Further, Delta's networked systems (many of them with unknown limitations) and operational environments, along with their interconnections in an institutionalized environment that was amassed over 70 years of operations, were vastly more complicated than the constituent agents and institutions of the Apollo 13—a relatively short-lived program.

However, no matter how dissimilar the computer technologies, or how much more complex Delta's situation when compared to Apollo 13, the broad risk management process was the same. A vulnerability in the critical infrastructure systems of each was

exposed to a threat that placed lives at risk; and, new controls were put in place to mitigate the risk under a crisis situation when time was running out. The management of the information security problem in each case was successful, and "proved itself a model of how to make life-and-death decisions."

The objectives of this final chapter are to summarize the results of the study of Delta, to consider study findings in light of relevant limitation, and to present further discussion related to theoretical implications and implications for information security practice. Recommendations for future investigations based on the findings of this study are included.

The aim of this dissertation was to investigate how complex organizations deal with problems in computer-based systems that affect the security of the information that they store and transmit, and to understand how environment influences their solutions. To achieve this objective, the study examined the *Y2K* compliance process at Delta, a complex critical sector organization and one of the nation's oldest commercial air transportation organizations, in order to explain compliance decisions in light of environmental factors, and to relate these decisions to information security.

Because of the size and complexity of the organization, and especially because of the nature of the expanding social environment that surrounded the management of Delta's networked information systems, institutional theory was viewed as a useful heuristic framework for investigating the research question and conceptualizing the analysis of the data.[140] A case study approach was employed to develop the evidence.

---

[140] Because of IT networks, the social environment included more users, with a wider spectrum of competencies, which are interconnected to and interact with more complex computer-based systems than in the recent past.

The study examined both primary and secondary sources of evidence. Archival documents pertaining to the Year 2000 Program at Delta, along with previously published materials, were examined to determine the *Y2K solution* in each of four core business areas. Year 2000 Program members, organization administrators, and others related to the Delta environment were interviewed, both to validate the archival records and to gain understanding of institutional influences (as revealed in the records analysis and as perceived by the informants).

Summary of findings

Delta's goal was "to simplify the technological infrastructure, improve efficiency and deliver state-of-the-art solutions for Delta's business needs" (Delta Air Lines, 1997, p. 15). This was a clear indicator of the expectation of Delta's management that the Year 2000 Program would improve the company's performance as a rational system. This dissertation affirms Delta's success in meeting its goal. The following is a summary of key findings.

First, with regard to theory, the research hypothesis stated that evidence would confirm a fit with an institutional model of performance; i.e., regulative, cultural, and / or mimetic mechanisms in Delta's environment relating to the ideas of new institutionalism (DiMaggio & Powell, 1983) would constitute the principal pressures that shaped *Y2K* solutions. The expectation of a match between the Delta Year 2000 Program performance and an institutional model was partially supported.

Institutional theory was supported in that business area solutions reflected evidence of incomplete rational evaluation and of mimesis. Specifically, at the outset a rational evaluation of consultants to lead the Year 2000 Program was curtailed by hiring

Feld, a consultant known to Grinstein through a previous working relationship. In addition, commercial software solutions were chosen based on what was available in the marketplace, not based on ideal solutions that might be achieved through customized design and coding. Therefore, rational choice was bounded, reflecting the ideas of Simon ([1945] 1976) and his notion of "satisficing," the ideas of North (1992a, 1992b) and his institutional economics model; and Cohen, March, and Olsen's (1972) garbage can model.

Given the chaos of the existing Delta systems, the limitations in resources, and the rush to reconstruct and to modernize, the choice of SAP modules for *Business Support*, and especially in *Operations*, may be seen as "solutions looking for issues to which they might be the answer" (Ibid.). Available commercial solutions and "best practices" are by definition mimetic notions, since obviously others have previously conceived and applied these software solutions. However, each of these institutional mechanisms limits an ideal solution by virtue of the fact of its generalized development.

A best practice holds aspects of both rational and institutional features. As a rational feature, an industry best practice is described as proven technology based on experiences in application that have shown to be effective in producing a desired outcome. As an institutional feature, a best practice is a fashionable management idea, often conceived by academics, promoted by management consultants, and adopted by organizational leadership. These application decisions are based on attempts either to improve efficiency and effectiveness, or to embrace the fad because they see it as validating their roles as leaders and innovators or as a means to career advancement.

> Academic writings, practitioner press, consultants and many formalized methodologies view technological and organizational planning as the objective collection, evaluation, and application of data in a rational manner to direct the planning process. In application, however, planners are often motivated by individual interests, maintaining appearances, and demonstrating superiority in knowledge and influence. (Tillquist, 2002, p.40).
>
> "The best-run businesses use SAP" (Sign in the Atlanta Hartsfield airport, 2007).

The use of COTS methodology for the solution process (BDM methodology), and the institutionalized thinking of the BDM consultants who assisted, is a similar mimetic action. This process obviously worked well enough, as evidence shows that the methodology and other outside influences brought rationality to the chaos. However, these sources may also have provided "blinders" to Delta's wider environment and its threats to the security of information systems.

Cultural effects associated with institutional theory were also evident in the processes—the program strategy, its adaptation, and its execution. The militaristic "command and control" style of the leadership was a direct result of military training and the flight operations culture, of work experiences as pilots or other military or airline positions.

However, institutional theory was insufficient to explain all aspects of the results. Indeed, there was strong evidence that supported the rival hypothesis that a rational-contingency model could explain solution choices. Pervasive throughout the Year 2000 Program were actions and communications that reflected a focus on goal orientation, reducing complexity, and increasing efficiency. A "best way" was configured at the outset based on a standard project methodology, and the organization adapted to contingencies along the way, principally confronting new learning about the problem and about the resources that were available to make the project function efficiently. The evidence in Delta's business area performance showed significant improvements in

efficiency and related cost reduction. Thus, both the institutional model and the rational model together helped to explain the *Y2K* solutions, supporting a melding of the two models, which is consistent with ideas of prior works (e.g., Greenwood & Hinings, 1996; Gupta, Dirsmith, and Fogerty, 1994).

Second, in accord with an institutional model, independent coercive relationships were expected to exist between institutional environments and Delta's business areas, wherein the rules and restrictive interconnections that applied within business area sectors would influence and constrain their decisions regarding changes to IT systems. Any potential for such an effect on a sub-system basis was minimized by the collaborative environment of the air transportation field, which exhibited a "collective rationality" reflecting the broader level of isomorphism. Specifically, cooperative arrangements existed among regulatory agencies, industry organizations, competitor airlines, airports, and various other groups that benefited Delta and all organizations that populate the air transportation field in executing the massive project. In this cooperative setting, a vast network of related organizations worked together to address the issues they shared with respect to *Y2K*. Recognition that all groups were key stakeholders undoubtedly made this cooperation both possible and effective.

Further, rather than being forced to comply with restrictive regulations, Delta, given its long history and the high esteem in which it was held by other relevant constituency groups, was able to provide influential leadership during the process of addressing the interorganizational, national, and global issues. As a result, Delta may be viewed as having been sufficiently powerful to be influential in creating and instituting structural practices in its environment, and thus was able to garner affirmation of its

legitimacy in the process. Although clearly a question for another study, the case inspired curiosity as to the uniqueness of the airline industry compared to other sectors in this regard, i.e., if other leading enterprises might be the main forces for collective behavior in their respective fields.

Third, in terms of the effect on security management, the result was as usual a tradeoff between increased functional efficiency on the one hand and increased security on the other. Tradeoffs will always be required among security, and functionality, and efficiency (Schneier, 2007).[141] However, neither Delta nor the sub-organizations considered adequately the impacts of solutions on information security. The institutionalized conditions of legacy systems and silo operations may have limited the ability of the Delta veterans to conceive of information security threats. However, the cognitive restriction seemed deeper than that. The organization also seemed to lack overt connection to the concept of information security in the Year 2000 Program, even as Delta evidenced a strong collective institutionalization of the concept of safety, which is a related concept to that of security.

In addition, market-driven incentives were not adequately supportive of information security, and this remains true today, although the situation is improving. The consultants and vendors working in the Delta environment were ill-equipped to consider information security in their processes. Historically, this aspect of software development and installation was not a part of the project methodology of consultants. Because of these inadequacies, business areas chose *Y2K* solutions that introduced security problems in order to capitalize on the opportunity for competitive advantages. In

[141] As Schneier stated, "Security costs money, but it also costs in time, convenience, capabilities, liberties, and so on."

eliminating the one vulnerability of the *Y2K* bug, a different set of vulnerabilities was introduced that related to the open environment facilitated by Internet protocols. Further, the standards in hardware and software that afforded efficient maintenance also provided the opportunity to exploit security flaws.

Lastly, and most importantly, examination of the Year 2000 Program revealed the existence of significant strategic leadership, which can be associated strongly with best practices in the methodology of IT development and project management, as well as the quality of leadership often found in military culture. The evidence for this strategic leadership was unmistakable. Competence in leadership and in information technology, as well as effectiveness in strategizing, understanding assets, and motivating others all worked together with remarkable effectiveness to achieve the goals of the project. An interesting question that will remain unanswered is as follows: *could the quality of leadership that was vital to the success of the Year 2000 Program at Delta have developed from within Delta's own ranks?*

Limitations

> It is not the fact that the old theory is strongly disconfirmed that makes a single case study so important; rather, it is its provision of new causal mechanisms in empirical accounts that fit the data at least once (McKoewn, 1998, p. 12).

The findings from this investigation must be considered in light of study limitations related to methodology and design. Its first weakness related to the choice of design. This investigation was a contemporary study of situated action, therefore suggested a case study strategy. However, many critiques assert that case study designs have numerous flaws, most notably with regard to problems with both internal and external validity (Collier, 1998). With regard to internal validity, the subjective nature of

case study designs has drawn criticism, especially with regard to data collection. In this case, the author was the sole researcher, who was responsible for both defining the key constructs and finding evidence related to those constructs among the data. The researcher brings inherent bias to observation, but must attempt to maintain detachment and objectivity as much as possible. In addition, among the variables were concepts that were difficult to measure. The *Y2K* solutions in embedded cases included changes to computer code, but may have included changes in attitude or understanding, aspects that are difficult to observe and to measure, and required interpretation while reading reports and interviewing people. In addition, there are numerous other opportunities for introducing ambiguity, for example through the statements of informants, whose memory or attitudes may affect their descriptions of what happened.

In terms of difficulties with external validity, researchers question the generalizability of the results of a case study analysis. Although there are always potential problems with the case study method, a strength of this method is its capacity to deal with complex variables, such as the influence of "institutional context," where quantitative measurement is difficult. The method is also an advantage when studying a subject such as the security of IT systems, where the same outcome (e.g., *Y2K* success) can be achieved though different paths "in which there may be no single non-trivial necessary or sufficient condition" (Bennett & George, 1998).

While the concerns with a case study design could not have been completely eliminated (Yin, 1994), a number of steps were taken to maximize the validity and reliability of the results. The internal validity was strengthened by establishing equivalent cross-case features and measures. Concerns about the internal validity of the project were

minimized further by the use of the comparative method, in which four business areas of the organization were compared on a number of key constructs. In addition, the constructs were carefully structured and carefully used in the analyses. Further, the attention to alternative explanations for identified causal relationships was another attempt to bolster the internal validity of the design (Huitt, 1999). Multiple individuals were interviewed within each of these business areas, and conclusions therefore were drawn about the nature of events based on all of their information considered together. The external validity of the investigation was enhanced by the attention paid to utilizing theory to explain the findings and conclusions, as doing so allows for greater transferability of the meaning of the results to other contexts. It has been purported that theory is the vehicle for generalizing a case study's results (Yin, 2003). Generalizability is also enhanced by the consideration for rival hypotheses. The analysis was accomplished via the use of two competing causal models, which were designed to understand the relative importance of factors such as condition of systems, and institutional factors as influences on business area *Y2K* solutions.

Further, the study design was operationalized in a fashion that would allow it to be reproduced in other organizations over time. The target case provided sufficient material that could permit reproduction, in that each sub-unit case contained the detailed history of one specific business area's program contribution. The fact that the sub-unit cases encompassed the entire organization and its core functions means that it is likely that the findings could be comparable to those gleaned from other large organizations and their systems in general; thus the results have the potential to be generalized to a large extent.

Another aspect of the design that is associated with multiple challenges relates to the use of a qualitative, rather than quantitative, approach to data collection and analysis. Measurement is a distinctly separate stage in quantitative research, whereas in qualitative research measurement issues are integrated into the data collection process (Neuman, 2000).

A second major limitation of the study related to the time gap between the Year 2000 Program and the conduct of the interviews. Because of the time delay, many people were gone from the company, and were not available for interview. Of those that were available and willing to contribute, some had memories that were less clear. Recall bias is one of the common challenges with retrospective reporting.

A third potential weakness had to do with the reluctance of some of the informants to disclose fully the processes and activities associated with the Year 2000 Program.

Implications for theory

This dissertation has presented a cross-disciplinary empirical study, bridging traditional information security disciplines with organizational analysis. Given the increasing importance of IT to the reliable functioning of organizations, and particularly those with critical infrastructure responsibilities, organizational analysis is an important part of the effective management of organizational risk. This dissertation has revealed the importance of consideration for institutions in understanding organizational actions related to information security management.

While the focus of the argument was on consequences of system changes for information security, another contribution to theory falls under the area of organization

studies. The argument included an expectation of institutional model compatibility, but as stated earlier, this expectation was supported partially. The results give rise to the notion that organizations, *within their social contexts*, are quite rational in their choices. This blur between the goal oriented actions and those that reflect institutional influences creates problems for prediction using one model or the other exclusively in describing a complex organization. An organizational analysis must consider the instrumental rationality of actions with consideration for institutional aspects.

A comparison of business area actions underscores a remarkable consistency in the nature of social contexts—the institutionalized nature of both the core areas of the airline business and the institutionalization of external structures related to IT systems. The IT field has constrained choices both by the nature of hardware and software products commercially available at any point in time, and by the mindsets that have developed over the history of computing and consulting engagements.

> … application and use of technologies shape the perceptions and attitudes through the social processes of legitimation, institutionalization, and practice (Klein & Hirschheim, 1989, quoted in Tillquist, 2002, p.41).

Technology is a tool for competitive advantage, particularly in the deregulated environment of air transportation. As the marketplace and competitors force reevaluation of solutions, these forces produce institutional choices (e.g., upgrades to remain competitive). The pace of technology changes means that incomplete information is continuously problematic. In order to evaluate options rationally (complete information), a "quiet time" for evaluation is required, but this has not been possible. The constraints of *Y2K* and competition, in addition to the pace of IT, did not allow the possibility for considering all alternatives at Delta.

The rational-institutional blur is demonstrated by the action of the U. S. government in creating the TSA and placing its agents in the midst of a well-oiled, highly institutionalized, and efficiency-focused organization such as Delta. In the short term, this action not only introduced inefficiencies, but also actually ran counter to the TSA mission of improving security by its lack of complete information about performing security-related duties. However, this government action brought considerable awareness to the threats and created a conceptual / cognitive relationship between the customer and his / her responsibility in the security process. That part was consistent with a rational-contingency model, but an analysis based on cost / benefit, or notions related to efficiency would not include it.

Implications for policy and practice

> Nowhere is the age-old struggle between convenience and security more pronounced than in the battle to secure the nation's skies (Scalet, 2003).

Information security issues have changed dramatically in recent years, but our societal perceptions and structures have not addressed this adequately. The attack on our country by terrorists in September 2001, and the subsequent investigation and analysis of evidence, revealed the inadequacy of our present defenses. Changed also are the issues specific to information security, both in perception and in fact. This research provided an examination of organizations within wider institutional environments to learn how such organization-environment systems shaped security solutions in the Delta organization.

For Delta, a critical infrastructure organization with a long history of operation, the potential for *Y2K* malfunction had been especially threatening. Not only had the organization confronted computer-based systems with *Y2K* issues, the company had been

concerned with the state of these systems and with improving their functioning for several years. Some might say that the inability to envision the damage that could be done by not placing IT investment at a high priority was the height of incompetence. However, those years had been focused on cost-cutting, not on investing in infrastructure, and the technology too had been evolving.

It did seem strange, however, for an organization so strongly focused on safety to have overlooked the potential for failure inherent in aging IT systems. A connection between safety and information security was clearly missing. Even Loy, first as head of the TSA from July 2002 then as the second-highest position in the Department of Homeland Security beginning in October 2003, did not articulate clearly the relationship between information technology and the safety of flight equipment and maintenance operations when he was asked about airline safety.

> In the old days it was a blur—9/11 clarified it. Safety is all about the equipment on board, the training of the pilots, the effectiveness of the flight attendants, whether the wing is going to fall off, if the rudder does what it's supposed to do. All those things remain the responsibility of the Federal Aviation Administration. The security piece is focused on how transportation security fits inside Homeland Security, which fits inside national security (Scalet, 2003).

Notwithstanding possible disconnects between safety and information security at Delta, the company invested heavily in its information technologies. Within a highly structured organization and process, changes were made across the enterprise that in retrospect could not have happened at a more propitious time. However, the decision to make these changes simultaneously with the process of eliminating the *Y2K* bug seemed suspect—complicating an already high-risk situation. The continuously changing IT environment suggests the need to assess organizational IT continuously, not waiting for a dire situation to force it. Only after the year 2000 rollover would Delta management

begin seriously to address the broader issue of information security, and then because of a subsequent dire situation.

A comprehensive strategy for information security

A disconnect exists between the institutional studies on information security and the apparent real world application. Delta's approach in the Year 2000 Program was in keeping with contemporary arguments for a holistic organizational approach to information security. However, as this study revealed, a holistic concept and approach in a pure sense was not possible in a large, complex organization under the circumstances associated with a security problem. Within a company-wide strategy, information security actions were delegated via tasks in individual divisions with their associated cultures, a very reasonable and effective approach in such a crisis. A company-wide strategy for longer term management of information security would have to include a more lasting solution.

Best practices in institutionalized environments often dictate how an organization applies information technology systems. Best practices are extremely helpful in the sense that they give rise to diffusion of effective and efficient techniques that have been tested in actual application. However, in the case of IT standards, best practices can only be as useful as the fit within the organization they are designed to serve.

> The purpose of any standard is to provide a kind of plumb line, and therefore that standard must be, "What is possible?" and "What is useful?" not, "what is somebody else doing?" (Hoag & Cooper, 2006).

How are practitioners and policymakers constrained by best practices that bring about overly complex enterprise solutions in organizations, and by current sectoral regulatory arrangements? If effective controls are to be promoted in our organizational IT

systems, the institutions and the mechanisms by which they can be changed must be understood. A technology plan for an organization cannot be comprehensive and effective without considering the players in the technology professions outside the organizational boundaries. The institutional environment must accept responsibility for more and more of the structuring inside the organizations toward improving security.[142]

> It makes no sense therefore unless the … profession outside … can be supported in this task by a whole new development of the local authority services (Powell, 1961).

The "Powell" who made this statement was concerned with the changes that were proposed to mental health organizations (facilities) in Great Britain. However, the idea is the same as the institutional changes needed to support air transportation organizations or any other entity that relies on information technologies as a critical part of its mission. Unless the supporting services of all kinds (governmental, industry, enterprise, and individual) are coordinated with the need for security and are supportive of this in their policies and practices, the mission will be a continuing failure. Because of issues of access, a security policy cannot be adequate unless there is understanding of the risks and the protection measures both inside and outside the organization boundaries.

Networks make all users participants in the solution, just as the traveling public is part of the aircraft security solution. The community of users must be willing and able to accept progressively more responsibility for information security, which is now seen as strictly the "tech support" job. The endeavor must be sustained by a widespread public understanding and resolve. Without this, the planners may plan and the administrators

142 The daylight savings time change is a recent example of policymakers having no clue about the threats to IT systems with respect to date / time issues. Systems administrators felt that the impact was "far far greater than Y2K" (Babington, 2007). A Forrester Research analyst estimated the cost of making computer fixes to manage the daylight saving time shift at more than $350 million for the 7,000 U.S. public companies (Lohr, 2007).

may administer, but the culture will continue to operate as though someone else is responsible.

How people envision the problem…

> Delta has designed a "solution that fits the problem" (Robb, quoted in Murray, 2002).

Even though considerations regarding new, complex, IT systems often point toward improved organizational performance, many in executive management have been reluctant to get involved with the decisions. The realities that installing such systems often bring with them are daunting problems: design, development, project management, implementation and security challenges, and of course not least—the problem of cost. In the past, knowledge of the systems had been relegated to the "geek squad" in the organization and to vendors and consultants, none of which considered the effects of changes on the total organization.

It has been said that how one envisions the problem dictates its solution (Dery, 1984). However, over the years Delta executives had envisioned the activities of Delta Air Lines and the use of IT systems differently. Dave Garrett (CEO, 1978-1987), said to have "despised technology," viewed Delta's activities as supporting a personal relationship between the organization and its customers. Allen (CEO, 1987-1997) also found no value in the use of computer-based systems. One informant reported that Allen did not use a computer, and in fact did not have one in his office. Another employee who had spent close to 10 years in the organization under Allen's leadership said that Allen felt it was better to use pencil and paper. He quoted Allen as saying, "[Computers] will slow down our work, and we have to get rid of them."

The unsatisfactory IT conditions that existed in the business areas at the start of the Year 2000 Program undoubtedly stemmed from the preferences of Delta's prior decision-makers. These executives and managers had not envisioned the extent of the possibilities for IT systems to improve safety and customer service, and ultimately for financial benefit. This must have made it difficult for the employees that reported to them to bring forth a business case for heavy investment in IT systems. One could speculate that the development of *TransQuest* was a way to remove the IT activities from within the core business areas not as a strategic economic move, but as a way to remove them from immediate view of the CEO.

Mullin, in contrast to Garrett and Allen, viewed the business as a "mass market business, driven by price."

> Real-time information is key to all of Delta's operations. The challenge is to get information from the source to the customer (Mullin, 2004).

Mullin's mass market ideas focused on the power of networked information technologies. Mullin was an agent for change. He led the extensive restructuring of the airline's operations, including its fleet and customer service operations. Of course, the implementation of the customer service restructuring came about via the *Y2K* transformation. Recall that one of Mullin's first acts after taking over leadership of the airline in 1997 was to hire Feld, and to assign him responsibility for the IT overhaul and creation of the Delta Nervous System.

Robb, CIO following Feld, referred to Delta as having a very complex business model.

> You can see the business context by looking at the technology. I have never seen a model this complex. Delta Technology's biggest job is integration of functional "silos," or "stovepipes." … There is a direct correlation with a business model in weaving technology (Robb, 2004).

Further, Robb envisioned Delta as a "unique real-time manufacturing operation," explaining that

> the product is delivered at take-off every 40 seconds. Other than FedEx, Delta is the only transportation company to apply a manufacturing business model.
>
> "To get that plane off there is a whole assembly process of not just getting the passengers and their bags to the right place, but the crews there, the right aircraft there, the meals, the fuel," says Robb. Delta serves 415,000 meals daily, uses 7.5 million gallons of aviation fuel, boards 109,000 bottles of water, brews 2,500lbs of coffee. The list goes on. These elements of the business all have to come together at the right place and on time on several thousand occasions every day (quoted in Murray, 2002).
>
> "What's unique about our process is that the customer really is right there in the middle of that manufacturing process," says Robb. "When it doesn't go well, it's really very visible. When it goes well, they probably just don't appreciate the complexity."
>
> In a true manufacturing environment, there is lots of instrumentation; Delta can't do exactly this, but similarly has constructed a unique technology solution. With the new solution, Delta is able to "adapt." In this manufacturing operation, the DNS operates like a trading floor. FAA provides flying "slots." A hundred airports are "wired together." ATPCO is the fare tracker.

Not only must an organization envision its problems productively, but its decision-makers must develop a common model, a model that supports the security of its information and an understanding of its institutional environment.

Capitalizing on institutionalized perceptions

The Delta case transcends its sector as a model for aligning IT to business strategy. Also, in revealing the value in "systems housecleaning" and in developing infrastructure systems that can "put information in the hands of those who need it." Such language that can serve to communicate this can be heard by all. In the case of information security and its connection to all who use computers, it may be more valuable to communicate using sector-specific language—in Delta's case, the language of aircraft and airspace safety.

> Perceptions of and attitudes about tasks, technology, and change are seen to be shaped by social influences and shaped by cues from one's social context … (Pfeffer &Salancik, 1978, quoted in Tillquist, 2002, p.41).
>
> Safety continues to be the foundation of everything we do; it is our single most important obligation to customers and employees (Grinstein, quoted in Delta Air Lines, 2004).
>
> [Airline] safety depends not only on new technology but also on the century-old concern of labor relations. Efficiency in the air has a lot to do with security provisions on the ground. … None of us is flying solo (Garvey, 2002).[143]
>
> The bottom line is to know your industry, your business and its processes and systems, says Walter Taylor, vice president of airline operations systems and year 2000 at Delta Air Lines. Establish a set of "guiding principles" such as "Safety will remain a priority" or "We won't inconvenience a customer," he says (Saia, 1999).

The mechanisms that support safety, institutionalized in the air transportation sector, offer significant benefits toward Delta's attention to traditional safety issues (thus public benefits in that regard), but its information security may be downgraded by them if not overtly connected. One idea is to expand the notion of safety to include an understanding of information security, which may gain the assistance of all users in managing the problem. Nowak (2004) talked about the culture at Delta and the lack of interest on the part of the typical user in addressing information security issues—the difficulty in changing the culture to recognize the importance of information security and the employee's contribution to it. Weill ("MIT's Weill on Leveraging Infrastructure," 2003) spoke about communicating infrastructure in business terms; Robb (2004) mentioned his success in communicating about information technology requirements in business terms. He presented a business case for maintaining his *Delta Technology* IT budget by using terms that were familiar to the Delta executives (Curley, 2004). If communication at Delta regarding information security were positioned in terms that

143 Jane Garvey was the head of the Federal Aviation Administration (FAA) during the *Y2K* event.

resonated with the notion of safety, maybe the notion and the cultural change could happen more naturally.

Rethinking the regulatory model

> As with safety issues, success for all carriers is paramount. One failure impugns the entire industry (Delta archive, "Delta Year 2000 Program Briefing Book," 1999, p. 26).

Obviously, the airlines have already developed an institutional framework that can be employed to support information security. This was evident in the sector rally around addressing the *Y2K* problem. How can other regulative environments take advantage of this?

To do anything substantive toward reducing vulnerabilities associated with information systems may take a complete rethinking of the regulatory models. A terrorist threat has a singular focus. In contrast, companies like Delta encompass a great amount of complexity, therefore, numbers of challenges in combating such threats to systems. Compromise is required in the strength of government regulation because of the plurality of values represented in systems operations, and understandings of the threats. The model provided by Delta shows industry level focus, where contributors understand both the goals and the technical aspects of the operational space. If continued at the government level, inefficiencies are introduced—policy makers cannot possibly stay abreast of the challenges in a timely fashion. Are the kinds of information security policies being deliberated presently *consistent with the model demonstrated by airline industry cooperation, or do we need to rethink this problem?* Homeland security is working top down, and they cannot know if what they are imposing will work until after it is implemented.

One can understand a lot about a person or an organization or a society by observing its budgets and expenditures. One may achieve a similar understanding about people and organizations and societies by observing the state of their IT systems. In an organization, if IT systems are streamlined, efficient, and adequately secured, the organization will function that way also. If IT systems provide adequate information security, organizational assets and operations have the best chance for survival. Observing the state of the Delta IT systems in 1997 revealed an organization that was in a mess. The housecleaning and modernization that was achieved through the Year 2000 Program has most likely enabled efficiencies that will not and maybe cannot be measured, but are inherent in almost everything that happens at Delta and with its customer / supplier interactions.

Suggestions for future research

> An institutional perspective supports a broader and longer view of organizational and social change. It encourages us not to restrict our attention to the legal or regulatory aspects of environmental controls, but to consider also the changing normative systems and cultural-cognitive frames. It also reminds us to be reflexive and put ourselves in the picture (Scott, 2000).

Computers-based networks are pervasive in our society. However, changes to the institutionalized attitudes about them have not kept pace with the evolution in technologies. Users remain passive consumers, and expect “tech support” to handle all issues. To increase the security of these systems, it is critical that we transform human attitudes and understanding in order to engage users in the active process of enabling information security and creating new solutions. Just as professional associations, the insurance field, privacy regulations, and business models have influenced medical practice, the vast numbers of organizations related to the information technology field

have influenced the practice and strategy for information security. More work needs to be done to engage with these issues in institutionalized environments.

This investigation can be replicated in other organizations. This dissertation provides a model for comparing similar processes in other comparably sized organizations. Thus, future studies can not only compare against experiences in other organizations, but against new security projects that can be carefully organized and controlled. For example, it could be important to contrast the *Y2K* response behavior of other organizations in the transportation sector that might be characterized as sharply different in terms of the organizations' longevity, complexity, or other relevant attributes.

> As aviation matures, there are compelling reasons why we must move beyond a manually operated Air Traffic Control. Traffic density is already straining the limits of what a human-centered control system can accomplish. For the foreseeable future there will be a human involved when needed, but the routine separation chores can be handled more easily and more efficiently by technology … As we move from an old fashioned manual method of sequencing aircraft toward an automated system we must plan for a larger number of aircraft. (Philips, 2000).

If Delta or another air transportation organization should choose to try to heighten awareness of information security as it connects with safety and survival, it would be interesting to understand how such awareness might affect solution choices in the future. It would also be interesting to compare the experiences in other organizations based on examination of military- vs. non-military-style leadership. Future analysis of individual perceptions might be beneficial for refining understanding, considering that these contrasting cultural conditions existed across the organization.

However, these contexts also point out the cognitive contexts that have focused more on efficiency, and flight and workplace safety, than on information security, and in fact, the meaning of information security had no immediate association for organization members within the context of IT systems apart from the now common association with

network penetrations by "hackers."[144] Yet, the *Y2K solution* choices altered the requirements for information security management.

Was this project a product of top management finally focusing on IT investment? If an information security issue (i.e., *Y2K*) elevated information technology to the forefront in this case and provided a catalyst for action to improve systems operation, can security policy be the driver again? A crisis environment has deep potential for advantageous positioning. In the case of external contingencies like *Y2K*, Robb believed that employees at *Delta Technology* worked *better* in an atmosphere of crisis. He expressed wonder about how a "crisis atmosphere" might be instilled in a "normal" project.

New perspectives on information security are required to comprehend what has happened in the past in order to make decisions that enable better policies for the future. Toward this end, the recent emergence of new technological infrastructures has created a need for collaboration among fields that have developed independent of each other—fields related to the technologies of information, and those related to their social contexts. One of the difficulties in accomplishing this has been the paucity of researchers who have knowledge in both areas, the technology area being a much faster-moving target than organization studies. This research was designed to contribute to such an integrated effort.

[144] The term "hacker" is a term that has become associated with malware, even though its original connotation is that of one who programs computers as a hobby rather than a profession.

APPENDIX A

CASE STUDY PROTOCOLS AND IRB APPROVAL

INSTITUTIONALIZED ENVIRONMENTS AND INFORMATION SECURITY MANAGEMENT: LEARNING FROM Y2K

A Comparative Study in a Critical Sector Organization

RESEARCH PROTOCOL

The problem: information security management in organizations

The societal problem

- Organizations are paying dearly to manage the information security problem, which manifests itself in not only fiscal expense, but also in loss of productivity and often valuable information for the organization, and in loss of reputation and trust by customers and constituents.
- The erosion of information systems security, which has been greatly facilitated by the networked environment, leaves our infrastructures vulnerable to compromise and therefore, compromises our national security.
- This erosion imperils the health and vitality of enterprise, and deprives the global community of a sure route to empowerment.
- The information security problem is amplified by the failure of organizations and the institutional environment to offer responses that can be seen as definitive and progressive.

The research problem

- Information security management is complex; it involves dealing with complex environments both inside and outside organization boundaries, and involves non-technical aspects as well as technical issues.
- Research on technical components, i.e., hardware and software, dominates the literature. Ways of envisioning and understanding the problem need creative expansion in the attempt to lessen its serious consequences.
- To manage the security of information and information systems effectively, an institutional infrastructure must be coordinated among organizational, social, and political rule systems.
- This dissertation fills a gap in the information security literature by focusing on institutional environments of organizations.

The project: a comparative study of the management of a security incident

"Institutionalized Environments and Information Security Management: Learning From *Y2K*" examines the process by which Delta Air Lines (Delta), a critical sector organization and one of the nation's oldest commercial air transportation organizations, dealt with the crisis of *Y2K*. The *Y2K* issue was this: many computer-based systems that relied on date calculations had been developed using two digits, rather than four, to specify the year. Because of the uncertainty regarding date calculations beyond 1999, no one knew whether systems would create erroneous results or fail completely without remediation or replacement of code that contained the "*Y2K* bug."

Y2K was a massive information security incident[1] that required the largest concentrated effort ever undertaken by the airline. To manage the remediation project, Delta set up a project management group, which included, among others, a representative from each sub-unit of the Delta organization. Its strategic plan for eliminating the security vulnerabilities associated with *Y2K* included certain activities to be performed in phases, i.e., according to a predetermined timeline of events, by each of the sub-units.

In 1997, Delta like many organizations was under pressure to deal with the *Y2K* bug. In that same year, Delta "launched a companywide Information Technology (IT) Transformation process," with a stated goal "to simplify the technological infrastructure, improve efficiency and deliver state-of-the-art solutions for Delta's business needs" (Delta Air Lines, 1997, p. 15). Between 1997 and 2000, Delta inventoried their IT systems, designed the new "transformed" systems, implemented changes (and decided on but deferred implementation of other changes) to its information systems, and to its organization structures and activities all while in the process of managing the organization's *Y2K* problem. However, as one might expect in a complex organization, these changes were not uniform across the organization; instead, they represented a variety of actions across sub-units (i.e., organizational divisions). Across sub-units, some actions may have been similar, but also some were different. Drawing from *Y2K*

---

[1] Like all system vulnerabilities, the complexity of systems environments rendered the *Y2K* bug difficult to eliminate. Preserving the *integrity* of information was the essential concern. However, the digital date coding scheme ultimately affected all of the features of secure systems (the confidentiality of information, its availability, and its integrity), and all system functions (its authentication scheme, its content, its accessibility, and its operations). Therefore, the integrity of the data affected the control and safety of critical infrastructure systems.

documentation, archival records, interviews, and a review of the literature, this study attempts to employ an institutional system model to explain what happened and why.

RESEARCH OBJECTIVE AND QUESTION

The objective of the study is to understand how institutionalized environments influence information security in large, complex organizations. The research question: *how did Delta go about addressing and solving the Y2K problem, an IT problem that affected the security of its electronically stored and transmitted information; and how did contextual conditions influence the solution?*

The structure of the design is based on the knowledge that Delta's sub-unit business areas arrived at different solutions for the same problem. To answer the question, two opposing organization theories are employed: institutional theory and rational-contingency theory. These two perspectives offer possibility for generalizing the theory to include other organizations. For example, if an institutional model fits the evidence, then this study will provide verification and replication in the context of the Delta setting the theory that an organization system performs based on other than efficiency (cost/benefit) criteria. In either case, the potential exists to demonstrate that institutional environments are important to information security management.

Theoretical foundations

Organization theories can explain relationships between forces in organization environments and observed actions of organizations, actions that can place the security of organizational systems at risk. Organizations are represented as "systems" where a conceptual boundary exists between activities that the organization controls and its external environment. Open system theories represent organization activities as extending into the environment outside organizational boundaries. Both technical and institutional aspects of the environment channel and constrain organizational performance. In the *technical environment* competition for resources and other contingencies potentially constrain efforts to maximize efficient or effective organizational performance. In the *institutional environment* organizations comply with rules and other institutional requirements in order to receive legitimacy and support, i.e., they compete for social fitness rather than economic efficiency. The institutional environment establishes social

norms and expectations of legitimate behavior, therefore, channels performance depending on restrictions imposed by laws[2] and other social structures. Institutional environments form the context within which technical resources are made available and legitimate. With respect to these technical and institutional environments, two organization theories, institutional system theory and rational system theory, are in conflict.

Institutional system theory (DiMaggio & Powell, 1983; Scott, 1992; Selznick, 1948) claims that (1) institutional environments influence organizational structure and operation; and, (2) via regulations and other pressures in the common space of an organization sector, organizations tend to become similar because of their efforts to be competitive and to maintain legitimacy.

The institutional system model portrays the Delta *Y2K* actions—and the development of the Delta *Y2K* plan—as a contextualized process shaped by institutional mechanisms, i.e., historical values, perceptions, and judgments, which in turn contributed to more explicit channeling provided by regulative mechanisms, technical resources, and other forces in the organization's wider environment. According to this theory, a sub-unit may have acted to satisfy values such as a desire for more modern equipment, for more management control, or because the resources were available to do it. The actions may have far exceeded the goal of eliminating the *Y2K* bug, and further may have served no verifiable contribution to the efficiency or effectiveness of the sub-unit activities. Ideas of efficiency may have been secondary to the larger attempt to position Delta as a more competitive, and legitimate player in the fast moving air transportation environment. If that were the case, differences across sub-units would have had their origins in the histories of the departments, and, more specifically, in the histories of the fields—i.e., wider sub-unit environments—represented by the respective divisions.

The rules and expectations associated with the wider environment represented by an organizational field [3] are manifestations of three broad institutional mechanisms:

---

2 A regulation may be assessed in terms of its ability to support an efficient outcome, e.g., tax incentives. However, from an institutional perspective a regulation is a product of a social system, values-oriented and may actually inhibit efficient operation.

3 An organizational field consists of communities of related organizations: organizations that produce similar services or products together with their suppliers, resource and product consumers, and

regulative, cultural, and mimetic[4] (Scott, 2001, p. 52). These categories Scott (1987) expanded from three to seven, describing more specifically the assortment of mechanisms that he observed in empirical literature.

Institutional mechanisms described as regulative:

1. Imposition by environmental agents in institutional sectors or fields with coercive power.
2. Authorization by superordinate unit, or authorizing agent.
3. Inducement by environmental agents in institutional sectors or fields lacking coercive power.

Institutional mechanisms described as cultural:

4. Bypassing of organizational structures to establish control in organizations through belief systems.
5. Imprinting of basic industry or sector characteristics at the time of their founding that tend to persist over time.

Institutional mechanisms described as mimetic:

6. Acquisition of structures and patterns by imitating the actions of other organizations.
7. Incorporation of environmental complexity into organization structures.

According to an institutional system perspective, institutional mechanisms shaped each sub-unit organization's respective sectoral environment. Therefore, these mechanisms contributed to its particular approach for *Y2K* project strategy and implementation.

Both rational and institutional system theories consider that organization structure and performance are vitally affected by environmental influences. However, for a rationalist, organizations adapt to environmental contingencies as they pursue a goal of efficient and effective operation. Rational system theory is a traditional approach to explaining the actions of a profit centered organization. Rationalists would argue that sub-units had freedom to choose their actions within the scope of their functional subsystems, and they did so based on economic principles.

---

regulatory agencies. Some organization fields are often identified by industrial sector.

4 Institutionalists claim that mimetic mechanisms are at work in situations whereby organizations are uncertain as to a course of action.

> … [T]he rational-contingency model views organizational actions as the result of choices made among a set of goals in an environmental context of constraints and opportunities (Drazin & Van de Ven, cited in Hall, 1996, p. 295).

A rational system perspective on Delta's *Y2K* actions would consider the *Y2K* compliance plan as a rationalized blueprint for achieving a predetermined goal. The scope of *Y2K* was precisely defined and organized. The division of labor and marching orders were decided. Each sub-unit contributed its part to implement the plan, improving the efficiency of operations in each case. A coordination mechanism provided integration of the parts. According to a rationalist perspective, the actions of the sub-units were a rational response to eliminate the uncertainty of *Y2K*, and their differences strictly related to the diverse activities that each sub-unit performed and the kinds of technical equipment required for supporting those activities. Any deviation from the goal was caused by technical environments and resource limitations. Evidence that the organization performed according to a rational system model would include factors such as:

1. the quantity and structure of the sub-unit labor force based on predictability of tasks
2. sub-unit focus on the singular goal of eliminating the complexity and uncertainty associated with the *Y2K* vulnerability
3. clear and certain means to achieve the goal
4. reporting/coordination mechanisms that enabled project integration and control
5. sub-unit decision-making based on efficiency criteria.

Hypotheses

To test these propositions, this investigation considers competing hypotheses that reflect the institutional system and rational-contingency system perspectives, respectively:

Hypothesis 1: the institutional system model: *The diverse Y2K solutions of Delta business areas can be explained as institutional responses to contextual conditions, which are related to sector-based institutional mechanisms.*

Hypothesis 1a: Business area solutions were institutional responses that reflected industry regulations.

Hypothesis 1b: Business area solutions were institutional responses that reflected existing inter-organizational relationships.

Hypothesis 1c: Business area solutions were institutional responses based on solutions of other organizations.

Hypothesis 2: the rational-contingency system model: *The diverse Y2K solutions of Delta business areas can be explained as rational responses to contextual conditions.*

Hypothesis 2a: Business area solutions were rational responses to technical system conditions.

Hypothesis 2b: Business area solutions were rational responses based on cost/benefit evaluations and availability of resources.

METHODS AND DATA

Methods

The research method is a retrospective, interpretive study of the environments of four sub-unit business areas as individual sub-cases. The unit of analysis is the organization. The study is a comparison of sub-unit *Y2K* actions and the possible factors that influenced those actions.

The first step is to develop the context and content of *Y2K* response actions of the Delta sub-units. The next step is to present rational system and institutional system explanations for the actions. The final step is to compare the sub-unit cases to determine whether the same relative causes can explain the differences in solutions adopted for dealing with the same problem.

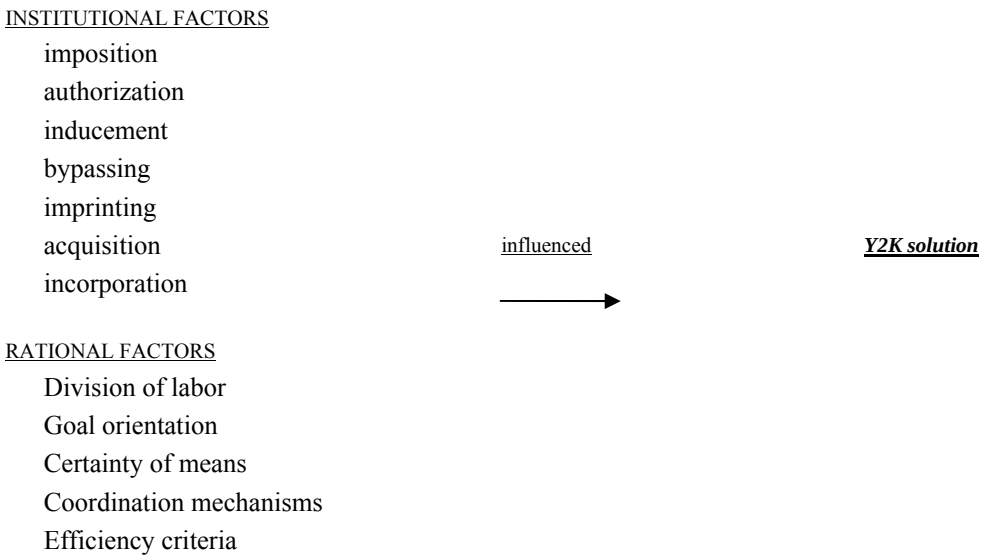
The method of analytic comparison (Mill's method of difference) [5] forms the basis for comparison, which systematically compares among the set of cases those that are similar with regard to outcome and causal factors with other sets that differ on outcomes and causal factors. The method enables finding cases that have the same causal factors and outcomes but lack a few key features, then through a process of elimination, locating factors common to all.

[5] Neuman (2000) describes Mill's logic. For further discussion, see Ragin (1987).

The investigative methodology includes comparison of the four business areas with respect to three variable constructs: *Y2K solution*, *environmental context*, and *response assessment.*

The dependent variable, *Y2K solution,* is defined as *changes to software systems in a functional business area of Delta over the period 1997-2003*.

An independent variable, *environmental context,* is defined as a set of conditions that existed in a business area-environment system and impinged upon the decision processes.



Data collection

A combination of data collection techniques will be employed in the study: (1) a search of *Y2K* documentation and archival records and, (2) interviews. As much as possible, sub-unit demographic data will be obtained from secondary sources. In order to confirm and elaborate on archival information, the investigation of *Y2K* documents will be followed by interviewing people associated with the project. It is expected that interviews will consist of at least 5 or 6 members of each of the target sub-units who were employees of Delta between 1997 and 2003. Participation will result in at most two interviews with each participant, a one hour interview, and possibly a short follow-on interview if clarification is needed.

Interviews will probe certain themes in an unstructured way. The themes support the test for sets of rival factors: institutional factors (categories of institutional

mechanisms: regulatory, cultural, and mimetic), and rational factors (categories pertaining to economic decision-making). Interviews will assist in understanding the issues that each sub-unit organization faced during the study period and how each organization went about addressing them. The categories will serve only as prompts in asking questions during interviews, and will not form part of survey instruments.

Confidentiality

The statements of the interviewees must be carefully handled, not only to protect their rights as human subjects, but also to ensure their validity. In individual interviews, informants may not wish to share certain items of information, items that could imaginably threaten employability (e.g., relating to division performance with respect to information security, relating to cultural, or other divides in their division, etc.). It is therefore important to follow procedures to keep such personal information confidential in this study. The data that is collected from an individual will be kept private to the extent allowed by law. These records will be kept in locked files and only the PI and dissertation advisor will be allowed to look at them. Names and any other facts that might point to specific individuals will not appear when results of the study are presented or published. Although identities will remain confidential, informants will be provided the opportunity to review any verbatim quotes.

A digital audio recording device will be employed in the interviews, if the informant is comfortable with that. Audio recording is not a requirement, but an aid to accuracy and to digital text conversion. If a recording device is used in the interview, audio files will be kept no longer than 1 year, and only the PI will have access to the files. They will be erased after the necessary information is collected from them.

ANALYSIS PLAN AND CASE STUDY REPORTS

To facilitate analysis, the documentation is first organized according to sub-unit, and then chronologically within each sub-unit to follow the phases of project development. Additionally, data is assembled that pertains to external organizations that played a role during the project. Results of case analysis will produce the following three tables:

Table 1: Y2K actions by sub-unit

Y2K ACTIONS	FINANCE	FLIGHT OPERATIONS	TECHNICAL OPERATIONS
Security practices			
Security policy			
Safeguards design			
Security clearances			
Employee monitoring			
Awareness program			
Risk analysis			
Security planning			
Disaster recovery planning			

Table 2: Manifestation of institutional factors by sub-unit

FACTOR	FINANCE	FLIGHT OPERATIONS	TECHNICAL OPERATIONS
Imposition			
Authorization			
Inducement			
Bypassing			
Imprinting			
Acquisition			
Incorporation			

Table 3: Manifestation of rational factors by sub-unit

FACTOR	FINANCE	FLIGHT OPERATIONS	TECHNICAL OPERATIONS
Sub-unit structure			
Goal orientation			
Certainty of means			
Coordination methods			
Efficiency criteria			

Case reports will be the multiple-case version of the classic single case (Yin, 1994, p.134), where four divisions (sub-units) of Delta represent embedded cases. The dissertation will contain a chapter covering the cross-case analysis and results.

THE RESEARCH SITE

Delta Air Lines is a large civil aviation organization with national and international operations. In 1997, some 8,600 Delta pilots were flying approximately 550 aircraft over national and international routes, and its total employees numbered over 63,000. In order to produce their finished product, which is safe and reliable transportation for people and freight, many parts of this complex organization must be working together: therefore, a system of reliable and timely information is vital to their business operation. The importance of safety and reliability of all commercial air transportation organizations has produced a number of agencies that provide regulatory oversight. From 1997 to 2003, the period during which the Delta *Y2K* actions were taken, a number of air transportation guidelines, professional certifications, and regulations existed that may have influenced the way divisions organized and developed its IT systems.

Table 4: Delta organization-environment complexity

Enterprises	**Contingencies**
Freight operations Delta DASH Passenger services Domestic International Charters Delta Shuttle Delta Express Code-share services Information Technology services WORLDSPAN *TransQuest/ Delta Technology* TIBCO, a *Delta Technology* Partner Communications services DeltaTel	Scheduling Airports Personnel Maintenance Partner airlines Weather Union activities Fuel cost Competitive market activities
Domestic and international operations	**Regulatory agencies**
Airports Other airlines Ownership Partnerships Alliances	Union Inter-industry Government Safety Security Financial Tax International

Table 4 continued

Resource dependencies	**Corporate compliance responsibilities** [6]
Customers	Antitrust
Suppliers	OSHA, Safety and health
Jet fuel	Federal Aviation Act
Aircraft	Environmental
Aircraft parts	Federal contract procurement policies
Food service	Copyright and other intellectual property
Human Resources	Political activity
Pay scale	Employee Retirement Income Security Act (ERISA)
Security clearances	IRS, foreign taxation
Qualifications	Securities and corporate governance
Personnel	Embargoes and trade sanctions
Airport flight controllers	Immigration (including employment of aliens)
Pilots	Foreign Corrupt Practices Act and other anti-bribery and anti-kickback laws
Mechanics	Use or sale of drugs or alcohol while on duty
Flight attendants	Falsifying company records
IT workers	Compliance with other laws and regulations
Computer-based systems (IT)	
Funding, financial operation	

Delta is an appropriate target for this study because:

- …the organization's operations depend on the reliable functioning and trustworthiness of networked information systems. Scheduling (time, place, date) of operations is critical; therefore, Delta's ability to comply with the directives of *Y2K* policy is related to its ability to continue to deliver service and to the ultimate survival of the organization.
- …as a large, complex organization, Delta characterizes the differentiated environments within which security mechanisms must often be implemented. Further, the environment of the organization may be characterized as simultaneously technical and institutional.
- …it is identified within a critical infrastructure sector.
- …the organization has detailed documented evidence of the *Y2K* compliance process.
- …the administration of the *Y2K* project was carried out in Atlanta; therefore, sources of information are convenient for the investigation.
- …access to the organization has been provided for purposes of this work.

In January 2004, early in the study design stage, access to the Delta organization was arranged by Leo Mullin, who served as Chairman and CEO of Delta during the years of the *Y2K* project. Mullin, who had resigned as CEO in December 2003, provided introduction to the employee who directed the project. Through this connection, extensive documentation of the *Y2K* project in the form of CDs and printed documents was made available.

[6] See "Corporate compliance is everyone's responsibility," 1997, p 10.

In 2006, this organization is a very difficult research site because of its bottom line—Delta reported a $2.6 billion net loss on $12 billion in revenue for the first nine months of 2005. In the attempt to reduce operating costs, layoffs and employee attrition have led to a workforce that has to shoulder more than its normal share of duties, therefore, has less discretionary time to spend with this Georgia Tech researcher.

More recently, access has been facilitated through the office of Jerry Grinstein, CEO and former Delta board member.

REFERENCES

Baskerville, R. (1997). New Organizational Forms for Information Security Management. *Computers & Security, 16*(3), 210.

DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review*, 48, 147-160.

Hall, R. H. (1996). *Organizations: Structures, Processes, and Outcomes* (6th Ed.). Englewood Cliffs, N.J.: Prentice Hall.

Neuman, W. L. (2000). *Social Research Methods: Qualitative and Quantitative Approaches* (4th Ed.). Boston: Allyn and Bacon.

Ragin, C. C. (1987). *The Comparative Method*. Berkeley, CA: University of California Press.

Scott, W. R. (1987). The Adolescence of Institutional Theory. *Administrative Science Quarterly*, 32, 493-511.

Scott, W. R. (1992). *Organizations: Rational, Natural, and Open Systems* (3rd Ed.). Englewood Cliffs, N.J.: Prentice Hall.

Scott, W. R. (2001). *Institutions and Organizations* (2nd Ed.). Thousand Oaks, CA: Sage Publications.

Selznick, P. ([1949] 1984). *TVA and the Grass Roots: A Study of Politics and Organization*. Berkeley, CA: University of California Press.

Yin, R. K. (1982). Studying Phenomenon and Context across Sites. *American Behavioral Scientist, 26*(1), 84-100.

Yin, R. K. (1994). *Case Study Research: Design and Methods* (2nd ed. Vol. 5). Thousand Oaks, CA: Sage Publications.

INTERVIEW PROTOCOL

Questions are organized according to the variables of interest to the case studies: informant history, Y2K solution, environmental context, and information security.

BY INDIVIDUAL
- History with the company
- Technology orientation
- Concept of information security

BY DELTA BUSINESS AREA
- *Y2K solution*
- *Environmental context*
  - Business area attributes
  - Sub-system environment
    - Cultural character
      - Military
      - Family
      - Technology orientation, concept of *Y2K*
    - Dominant fields
    - Regulative environment
- *Y2K* process - management & activities

INDIVIDUAL

*I1: How long have you been (or were you) employed by the company? Please tell me about your job.

*I2: What was your position at Delta during the period (1997-2003)? Did you have a specific role in the Year 2000 Program? … in one of the Portfolio, or Renewal groups?

The next questions relate to -- how the Y2K event became the focus at Delta, how the threat was understood.

*I3: Can you tell the story leading up to addressing the Y2K event at Delta?

When did you first become aware that Y2K was something Delta was going to have to deal with? How did the project start at Delta?

What was the general perception of employees about Y2K?

What did you understand the ultimate outcome to be?

*I4: If *Delta Technology* employee …

One of the pieces of information that I am curious about is the use of the term "IT Transformation." I have assumed that referred to the new DNS architecture and the

renewal of systems, but now I read that "IT Transformation" also relates to an organizational restructuring at *Delta Technology*. Were you there when this restructuring took place?

*I5: Do you have experience in other organizations? What about other Delta divisions?

If yes:

Probe different assignments in Delta. Which divisions? … terms of duty in those posts? …reported to whom? Can you describe the size of the departments? … any other characteristics? How were the departments structured?

*I6: Did you routinely interact with employees in other divisions as a part of your job? What aspect of your job created the need for interaction?

If so,

what did you notice about attitudes toward computer use? Did most employees use a computer to perform their jobs during Y2K? Has computer use changed since Y2K?

BUSINESS AREA

Y2K solution

*Y1: What changes were made in computer systems in your business area beginning with the Year 2000 Program? Can you describe particular actions or decisions?

Environmental context

REGULATIVE MECHANISMS

Addressing authorization: professional accreditations and standards of performance

*A1: Are professional certifications or educational backgrounds important to advancement in your business area? Are certifications required in certain instances? What organizations or agencies supply these authorizations?

*A2: Do standards of performance exist in your business area that are based in compliance with laws or regulations? … outside contracts? … professional standards?

*A3: Did organizations offering professional accreditations and standards of performance weigh into decisions regarding Y2K solutions? If so, how?

Addressing imposition: compliance obligations

*A4: What laws or government agencies regularly demand the attention of your business area? Is your business area subject to laws or regulations that differ from other business areas? If so, please describe the nature of the regulations. Were these same regulations in effect during Y2K?

*A5: What makes your business area comply with rules? Is coercion involved? Is it the threat of fines or other enforcement mechanisms?

*A6: What is your attitude toward government rules and regulations? Do they serve a useful purpose in your opinion? What regulations cause particular hassle or stress?

*A7: What other kinds of rules is Delta or your business area especially attentive to?

*A8: How much does your business area rely on outside advice for expertise on regulations and/or compliance reporting?

*A9: Do you think that regulations and rules affected the IT effort—either helped or hindered? (e.g., Specific requirements for Y2K compliance? Regulations in the air transportation sector? Other institutional factors?)

Addressing inducement: affiliations

*A10: What outside organizations does your business area interact with? What is the nature of the relationship(s)? e.g., suppliers, partner organizations, contractors. What relationships cause particular hassle or stress? … make your work easier?

*A11: Were Y2K guidelines or mandates provided by other organizations? Did protocols (e.g., output formats) or other technical issues dictate solutions in some cases?

*A12: Were there security issues with regulatory, partnership arrangements, rules, or other conditions during Y2K?

*A13: What different types of organizational relationships have employees relied on for help with complex systems problems? (within the organization? external relationships, e.g., paid consultants, professional organizations, personal friends, listservs, etc?).

CULTURAL MECHANISMS

Addressing bypassing: routines and familiarity with systems and practices

*B1: What kinds of activities are carried out in the business area(s) where you worked during Y2K? How would you describe these activities compared to other business areas at Delta (relatively stable, continuously changing, complex, critical, high or low pressure)?

*B2: Is there an emphasis on standard ways of performing? Do you have freedom in the way you perform your duties? What about the business area as a whole?

Addressing imprinting: how the business area has always done things

*B3: When people are hired at Delta in your business area, how do they learn what they need to know in order to advance in the organization? (Examples?)

*B4: In all organizations, there are groups or individuals that influence what gets done and how. What individuals or groups do you believe have the most power at Delta (outside the company officers)? What business area? What groups have the most power within your business area? Has this changed over the years?

Addressing imprinting: historical precedence favoring particular solutions (includes aspects of culture and their effects on group dynamics)

*B5: Tell me about the history of your business area within Delta.

*B6: Much has been written about the culture at Delta, calling the organization a family. Why do you think people identify it that way? How does this affect the way things get done?

*B7: In your opinion, do cultural separations exist within the company, e.g., older vs. younger, employees with military vs. non-military backgrounds, technical vs. non-technical, or racial divides? Are there business areas where a certain demographic predominates?

*B8: Did you serve in the military? If so, does your military background influence how you think about your job or how you perform your duties?

*B9: Are there other employees in your business area that have military experience? How many would you estimate? (As a percentage of the employees?)

*B10: Please describe how employees in this business area have used computers or computer-based systems. Did you use a computer to perform your job during Y2K? What is your attitude about computer use? Has your computer use changed since Y2K?

*B11: How did you usually bring up issues or problems with a computer system? Did a central computing group handle problems? Do you have tech support people in your business area? How much access do individuals have to Delta systems? Was it the same before Y2K?

*B12: I'd like for you to think about the different types of systems problems that members of your business area have encountered that required expertise beyond the normal capabilities of the group. Were there existing organizational relationships that the group called on? How would you describe each of the relationships to your business area?

*B13: Do you believe that the Y2K process was managed adequately? If you could, is there anything you would change about how your business area responded to the challenges of Y2K compliance?

MIMETIC MECHANISMS

Addressing acquisition: copying other organizations

*C1: Did the practices or experiences of other organizations (e.g., competitors or professional associations) weigh into the decisions of your business area during Y2K?

*C2: Did it seem to you that there was uncertainty concerning how to achieve Y2K compliance in your business area? Please describe.

*C3: How much, if any, did your business area rely on outside expertise for recommending Y2K solutions? Were outside organizations involved in these actions? If so, how did they influence what was done?

*C4: Did the popularity of software products in the marketplace matter in the decision process? Were any systems chosen because they were considered “best practices”?

Addressing environmental incorporation

*C5: Are there groups or individuals in your business area that have responsibility to manage issues with outside entities or affiliations? How do they fit in the organization structure?

*C6: What functions in your business area exist because of a process that is interactive across an external organization boundary?

RATIONAL MECHANISMS

Addressing organization: size of workforce, division of labor, coordination mechanisms

*D1: Tell me a about your business area organization and the organization of the Desktop Systems Project team? (e.g., How many employees? How was it organized? Was there a clear chain of command? At the beginning of the Y2K project, how did the systems in your business area communicate and contribute to the rest of the enterprise?)

*D2: How is your business area organized? Would you say that the structure represents a clear chain of command? Alternatively, is there a more informal way that things are done here?

*D3: Describe the characteristics of your business area. How is it structured? How many employees? Particularly specialized functions compared to other business areas?

Addressing goal orientation

*D4: It seems to me that there were multiple goals for the Year 2000 Program, and the IT transformation project. What was the goal (or goals) of your business area?

Addressing effectiveness of planning and strategy

*D5: How much strategizing was done at the business area level? Did employees understand the function of the IT systems as well as the DT employees?

*D6: Did the PMO, the CIO, or the IT Board dictate solutions at any point? If so, did this create a problem?

*D7: Do you believe that the planning and strategy for the Year 2000 Program was sufficient? Was anything unexpected or unplanned that caused deviation from the Program master plan?

Addressing operating efficiency

*D8: After replacement systems were installed, did they bring the expected benefits? Were there unexpected consequences?

*D9: Did the IT changes contribute to productivity or operating efficiency? If so, how? Were contributions to efficiency part of the original goal? Do you believe that changes contributed to productivity or did they add extra burdens in any way?

Addressing decision criteria

*D10: What do you think most Y2K teams worried the most about? … money, security, functionality, … something else?

*D11: Do you believe that choices of particular systems replacements were based purely on cost/benefit? What other considerations might have weighed into decisions?

*D12: Hindsight being 20/20, would you like to have the freedom to go back and make a different decision on any aspect?

*D13: Do you believe that business area decisions during Y2K were based on cost/benefit or some other criterion? I know that presentations were made concerning Y2K recommendations that required a cost/benefit analysis. Did this analysis actually influence the decisions that were made?

*D14: Given the focus of your business area activities, do you think that your administrators made decisions differently from those of other business areas regarding Y2K compliance?

Addressing technological and organization complexity

*D15: What were the technological and/or organizational complexities that challenged your efforts or those of your business area?

Information security

Questions addressing the concept of information security, level of awareness of information security in the organization–understanding of specific threats and vulnerabilities, involvement of organizational leaders and members in security processes, and the contribution of organizational and technological complexity.

Addressing information security understanding: the concept and awareness

*E1: How do you define information security? Can you describe a digital signature? …What does encryption mean?

*E2: How does security relate to safety?

*E3: What was your understanding of the Year 2000 Program as related to information security? Do you remember a part of the Program that specifically addressed information security? Do you remember meetings where information security was discussed? How was information security being addressed?

*E4: How do you feel about information systems security at Delta? During the Year 2000 Program, was there an awareness of information security at Delta beyond just doing a job? What did you learn about security during Y2K?

*E5: Does Delta have an information security policy? Do you have a clear understanding of what is and is not allowed? Have you received information security training? If so, how and when was the training administered? Is this different from the way your business area operated before Y2K? What jobs do the employees in the information security area of Delta (*Delta Technology*) perform?

*E6: Has there ever been an instance of insider attacks or mistakes that compromised the security of Delta's systems? What security routines are practiced here?

Addressing information security strategies: understanding threats and vulnerabilities, leadership and security focus

Addressing information security consequences: complexity

*E7: Did security issues change following installation of new systems?

*E8: Is information security better now than before the Y2K event? If so, to what do you attribute the improvement? If not, what happened that caused the negative impact?

*E9: If you could, is there anything you would change now about how decisions are made in your business area regarding systems issues or regarding information security?

Georgia Institute of Technology

Office of Research Compliance
Atlanta, Georgia 30332-0420 U.S.A.
PHONE 404-894-6944
FAX 404-385-2081
irb@gatech.edu
iacuc@gatech.edu

Protocol Number: H06133
Funding Agency: N/A
Review Type: Expedited, Category 7
Title: Institutionalized Environments and Information Security Management: Learning from Y2k
Number of Subjects: 25
Number Enrolled: N/A

June 12, 2006

Hans Klein
School of Public Policy
0345

Dear Dr. Klein:

The Institutional Review Board (IRB) has carefully considered your proposal referenced above. The proposed procedures afford reasonable protection to the human subjects involved and therefore you are granted approval.

Research qualified for expedited review in accordance with federal expedited category # 7.

Your approval and stamped consent form are effective **May 25, 2006** with an expiration date of **May 24, 2007.** Thereafter, continued approval is contingent upon submission of a continuation form/progress report that must be reviewed and approved prior to the expiration date.

Approval is contingent upon your agreement to obtain informed consent from your subjects, to abide by the Georgia Institute of Technology Assurance of Compliance for the Protection of Human Subjects, and to keep appropriate records concerning your subjects.

You are required to submit to the IRB for review any changes in procedures involving human subjects prior to the implementation. Any serious reactions or unanticipated problems must be reported immediately to the IRB.

Please note that all correspondence or e-mail you send to the IRB regarding this topic must include the full title and Protocol Number (shown in the upper right corner of this letter).

If you have any questions concerning this approval or regulations governing human subject activities, please feel free to contact me at 404/894-6942.

Sincerely,

Melanie Clark, CIP
IRB Administrator

Enclosure
cc: Dr. Phil Sparling, IRB Chair

INSTITUTIONALIZED ENVIRONMENTS AND INFORMATION SECURITY MANAGEMENT: LEARNING FROM Y2K

Invitation to participate

Dear <insert Delta division name>,

I am a PhD candidate in Information & Communication Policy at the Georgia Institute of Technology. I am writing to invite the participation of your division in my dissertation research, a study that examines the influence of sub-unit environments on information security actions at Delta during Y2K. I hope to include 5 or 6 members of your division who were employees of Delta in the 1997-2000 time period.

Participation will consist of one short interview (at most two, in the case of need for clarification or follow-on questions) from each participant. I hope to interview an administrator, a division representative to the Y2K project PMO, two people with particular technical skills, and two people who played roles but not as technical contributors. I would like to conduct the interviews at your office location, in which case I plan to exercise minimum disruption to normal work activities. There is no obligation associated with funding for this project that compromises the objectivity or confidentiality of the study. Unless I am directed differently, I will identify your division in my research report. However, the confidentiality of individual participants will be expressly protected. The attached summary provides information about the research project, which has received Institutional Review Board approval from Georgia Tech.

Please do not hesitate to contact me if you require more information. Also feel free to contact my advisor, Dr. Hans Klein. You may reach him by phone at (404) 894-2258, or by email at hans.klein@pubpolicy.gatech.edu. I hope that I will have the opportunity to meet with you and with members of your organization.

Sincerely,

Pam Hassebroek

PhD Candidate, School of Public Policy
Georgia Institute of Technology
Atlanta, GA 30332-0345

http://www.spp.gatech.edu

Email: pam.hassebroek@gatech.edu

Enclosed: research summary

INSTITUTIONALIZED ENVIRONMENTS AND INFORMATION SECURITY MANAGEMENT: LEARNING FROM Y2K

A Comparative Study in a Critical Sector Organization

SUMMARY

Computer-based information and communication technologies have become indispensable components of modern organizations. However, historical evidence shows that both the reliance on computer-based systems and their pervasive use have created new threats to organizational assets and infrastructure systems. Caused by the growing complexity and proliferation of these systems, their vulnerabilities have outpaced the means for making them adequately reliable and secure.

Because of the global networks over which electronic information travels, a great deal of current discourse has identified environments as a source of information security problems. Further, among environmental sources, many of the security problems are non-technical—resulting from the lack of harmony in legal systems, and the cultural differences that complicate operations of global organizations, among other issues.[1] However, historically, efforts to improve the security of computer-based systems have focused on technical components, i.e., hardware and software. Researchers and practitioners now understand that non-technical issues are significant—equal to if not more important than the technical issues, and that those at the environmental level are especially difficult to manage. Yet, very little empirical research exists in the non-technical-environmental area of information security. Therefore, helping to fill this gap, the purpose of this theoretically-based study is to understand ways in which wider environmental contexts shape security actions in organizations.

The focus for the research is Y2K. In the late 1990s, organizations tackled an information security problem of unprecedented scale. A small detail written into the code of computer-based systems before the year 2000, often called the "Y2K bug," emerged to create a worldwide crisis. Different from most crises or other failures, the Y2K bug affected not just a few isolated organizations; a vast number of organizations required changes to systems during the same period, and their networked environments complicated the process. At best, the Y2K problem represented a potential interruption to the normal workflow of an organization. At worst, the problem jeopardized the reliability and the ultimate safety of critical infrastructure operations worldwide. The successful elimination of the Y2K vulnerability provides a model to study how organizations contend with problems affecting the security of electronically stored and transmitted information.

Employing a comparative-case method and applying concepts from institutional theory, the study explains the variation in 1997-2000 Y2K compliance actions among three divisions of Delta Air Lines, Inc. (Delta), a complex U.S.-based transportation organization. Data for the study are archives, and personal interviews with individuals, related to the Delta Y2K project. Results can have implications both for policymaking and for future research in the field of information security.

---

1 "Non-technical" security management issues include, for example, laws, policies, education, etc.

Georgia Institute of Technology

RESEARCH CONSENT FORM

Principal Investigator:
Pamela B. Hassebroek

Project title:
Institutional Environments and Information Security Management: Learning from Y2K

You are being asked to be a volunteer in a research study of the Y2K compliance process. The principal investigator, Pam Hassebroek, is a PhD candidate at the Georgia Institute of Technology in Atlanta, GA.

Purpose: The purpose of this study is to understand factors that shape information security actions in organizations. The successful elimination of the Y2K vulnerability provides a model to study how organizations contend with problems affecting the security of electronic information, and what factors influence actions. Historically, security strategies have focused on hardware and software. Now, researchers and practitioners alike understand the need to consider other factors that lack empirical investigation.

Participation: An individual is eligible for participation in this study if he/she were a Delta Air Lines or Delta Technology employee, contractor, or consultant during the years 1997-2000. Members of six organizational divisions at Delta are being interviewed for this study. Participants also include members of the Y2K project management office (PMO), and corporate administration.

Procedures: If you decide to participate in this study, your part will involve one personal interview (at most two, in the case of need for clarification or follow-on questions), which will last approximately one hour. The interview will likely be conducted on-site at your place of business and in a manner to minimize disruption to normal work activities. During the interview, you will be asked questions about your experiences during the course of the 1997-2000 Y2K compliance effort. I plan to employ a digital audio recording device in the interview. Audio recording is not a requirement, but merely an aid to accuracy and to facilitate digital text conversion. Recordings will be erased upon their conversion to text. If you prefer, the interview will be conducted without recording it. Furthermore, although your identity will remain confidential, you will have the opportunity to review any verbatim quotes if you choose to do so. You may also request a synopsis of the completed study.

Risks/discomforts: There are no known risks associated with your participation.

Benefits: You are not likely to benefit directly in any way from participating in this study. However, through your participation and that of others, the findings of the study may provide indirect benefits (to all computer users).

Compensation to you: There is no compensation for participating in the study.

Confidentiality: The following procedures will be followed to keep your personal information confidential in this study: The data that is collected about you will be kept private to the extent allowed by law. To protect your privacy, your records will be kept under a code number rather than by name. Your records will be kept in locked files and only the principal investigator and dissertation advisor will be allowed to look at them. Your name and any other fact that might point to you will not appear when results of this study are presented or published. If I employ a recording device in the interview, I am the only person who will

Consent Form Approved by Georgia Tech IRB: May 25, 2006 - May 24, 2007

have access to these audio files. They will be erased after the necessary information is collected from them.

Costs to you: You will incur no financial obligation as a participant in the study.

Participant rights:

Your participation in this study is voluntary. There is no obligation to contribute to this study if you don't want to.
You have the right to change your mind and leave the study at any time without giving any reason, and without penalty.
Any new information that may make you change your mind about being in this study will be given to you.
You will be given a copy of this consent form to keep.
You do not waive any of your legal rights by signing this consent form.

Questions about the study or your rights as a research participant:

If you have questions about the study, you may contact the principal investigator, Pam Hassebroek, at (404) 233-7910 or at pam.hassebroek@gatech.edu. Dr. Hans K. Klein, advisor for this research, may be reached at (404) 894-2258 or at hans.klein@pubpolicy.gatech.edu. If you have questions about your rights as a research participant, you may contact Melanie Clark, Georgia Tech Institutional Review Board, at (404) 894-6942 or at melanie.clark@osp.gatech.edu.

If you sign below, it means that you have read the information given in this consent form, and you would like to be a volunteer in this study.

_____
Participant Name

_____
Participant Signature Date

_____
Name of Person Obtaining Consent

_____
Signature of Person Obtaining Consent Date

APPENDIX B

DELTA CORPORATE ORGANIZATION

Effective August 14, 1997, the Board of Directors (Board) elected Leo F. Mullin as the Company's President and Chief Executive Officer and a member of the Board. … The Board also elected Gerald Grinstein, a current member of the Board and former Chairman of Burlington Northern Santa Fe Corporation and Western Air Lines, Inc., as Non-Executive Chairman of the Board; Maurice W. Worth, a Delta veteran of 36 years, as Chief Operating Officer … (Delta Air Lines, 1997, p. 268).

DELTA ORGANIZATION

Non-executive Chairman of the Board, Gerald Grinstein
Chief Executive Officer, Leo F. Mullin
President, Leo F. Mullin
- Chief Operating Officer, Maurice W. Worth
- Exec VP - *Operations*, Harry C. Alger
- Exec VP - Marketing and Chief Marketing Officer, Robert W. Coggin
  - Sr. VP - Personnel, Robert G. Adams
  - Sr. VP - Sales and International, Vincent F. Caminiti
  - Sr. VP - Cargo, W. E. Doll
  - Sr. VP - Airport Customer Service, Vicki B. Escarra
  - Sr. VP - General Counsel and Secretary, Robert S. Harkey
  - Sr. VP - Corporate Planning and Information Technologies, Paul G. Matsen
  - Sr. VP - In-Flight Service, Jenny R. Poole
  - Sr. VP - Finance and Chief Financial Officer, Thomas J. Roeck, Jr.
  - Sr. VP - Corporate Communications, Thomas J. Slocum
  - Sr. VP - Technical Operations, Ray Valeika
  - Sr. VP - Government Affairs, D. Scott Yohe
    - VP - Corporate Safety and Compliance, Malcolm B. Armstrong
    - VP - Delta Express, W. E. “Skip” Barnette
    - VP - Public Affairs, Harold L. Bevis
    - VP - Properties and Facilities, John W. Boatright
    - VP - Consumer Marketing, Gayle M. Bock
    - VP - Delta Staffing Services, Business Unit Development, W. Martin Braham
    - VP - Flight Operations, Richard E. Colby
      Controller, Hiram A. Cox
    - VP - Marketing Development, Mark A. P. Drusch
    - VP - Atlantic/Pacific Business Unit, Stephan J. Egli
    - VP - Maintenance: Aircraft, Michael S. Ellenburg
    - VP - Personnel Relations, Terry M. Erskine
    - VP - Reservation Sales and Distribution Planning, Lee A. Macenzak
    - VP - Maintenance: Engine and Component, Harold G. McDonald
    - VP - Personnel Benefits, Leon A. Piper
    - VP - Financial Planning and Analysis, Edward H. West
    - VP - Community Affairs, Michael M. Young

Source: Delta Air Lines (1997). 1997 Annual Report.

Table 70: Committees of the Delta Board of Directors

EXECUTIVE COMMITTEE	AUDIT COMMITTEE	FINANCE COMMITTEE
Mary Johnston Evans, Chairman	Jesse Hill, Jr., Chairman	R. Eugene Cartledge, Chairman
Edward H. Budd	Henry A. Biedenharn, III	Edwin L. Artzt
R. Eugene Cartledge	James L. Broadhead	Edward H. Budd
Gerald Grinstein	Mary Johnston Evans	George D. Busbee
Jesse Hill, Jr.	Peter D. Sutherland	Gerald Grinstein
Leo F. Mullin		

PERSONNEL AND COMPENSATION COMMITTEE	BENEFIT FUNDS INVESTMENT COMMITTEE
Gerald Grinstein, Chairman	Edward H. Budd, Chairman
James L. Broadhead	Edwin L. Artzt
R. Eugene Cartledge	Henry A. Biedenharn, III
Mary Johnston Evans	Jesse Hill, Jr.
	Andrew J. Young

Source: Delta Air Lines (1997). 1997 Annual Report.

Leo F. Mullin

Leo Mullin served Delta as Chief Executive Officer (CEO) from 1997-2003. Mullin has been called an agent of change, and may be viewed as an institutional agent. He played a "fundamental role in creating and shaping the character and identity of [Delta]" (Scott & Christensen, 1995, p. 149) from August 1997 until December 2003, when he announced his intention to retire. Between 2001 and 2003, the chiefs of eight of the top nine airlines had been replaced (DiCarlo, 2004). A number of sources have pointed to Mullin's role in enabling the creation of 40 different Internet-related programs and the radical improvements in how Delta related to customers, business partners, and employees (Corcoran, 2000).

Gerald Grinstein

Gerald Grinstein became CEO of Delta in January 2004 after Mullin stepped down. Previously, Grinstein had served as CEO of Western Airlines of Los Angeles, California. When Western merged with Delta in 1987, he was appointed to the Delta Board of Directors, a position he had held continuously after that. From 1985 to 1995,

Grinstein was CEO of Burlington Northern Railroad (BN). In this position, he led the organization through a merger with Santa Fe Railroad, forming the BNSF Railway. As CEO of Delta, Grinstein led the organization through a cost management process in the attempt to avoid bankruptcy. Delta ultimately filed for bankruptcy protection in 2005, in part because of unusually high fuel prices.

Figure 7: Delta corporate leaders in 2004

From left to right: Leo F. Mullin, Chairman, Gerald Grinstein, CEO, John F. Smith, Jr., Presiding Director

APPENDIX C

DELTA TECHNOLOGY ORGANIZATION

Table 71 shows the organization of Delta Technology during the Year 2000 Program. Note that the VP – Air Operations Portfolio also served as the Director of the Year 2000 Program.

Table 71: *Delta Technology* organization

Chief Executive Officer, Charlie Feld – The Feld Group
VP - Chief Financial Officer, David Pittman
VP - Human Resources, Greg Tavohnen

APPLICATION PORTFOLIOS	TECHNOLOGY PORTFOLIO
VP – Customer Portfolio (customer functions), Keith Halbert - The Feld Group	Sr. VP – Technology Portfolio
VP – Air Operations Portfolio (flight operations functions, pilots, flight attendants, mechanics), Director Year 2000 Program, Walter Taylor	VP – Common Services, Wayne Hyde
VP - Business Support Portfolio (internal audit, finance, legal, HR functions), David Pittman	VP – Engineering, Paul Millard Desktop Strategy Project leader, Tim Mitchell
VP - Revenue Portfolio (sales, marketing functions), Vince Accardo – The Feld Group	VP – Systems Operations, Harry Richardson (beginning in 2000)

Charlie Feld

Feld served as interim CIO of Delta and CEO of *Delta Technology* from 1997 through 1999. During that time, Feld was responsible for the development and operations of *Delta Technology*. While in this role, he was awarded the 1998 "CIO of the Year" award from the state of Georgia. *Delta Technology* received the 2000 Smithsonian Award for Technology Excellence for the CustomerCare system, which was developed and implemented under his leadership. After January 2000, Feld was involved with Internet related aspects of IT at Delta before leaving in 2001.

Previously, he was employed by Frito-Lay in 1981 as CIO with responsibility for implementing an integrated computer system that connected all departments into a common communications and data network. Feld began his association with Frito-Lay in 1970 as systems engineer for IBM on the Frito-Lay account, playing a key role in developing the company's computer network over an 11-year period.

Feld founded The Feld Group in 1992, where he built a team of IT consultants that helped to transform IT in a number of organizations, including Burlington Northern (BNI) where he met Grinstein, then CEO of BNI and a member of Delta's Board of Directors. As CIO at BNI, Feld led the team managing the massive integration of the Burlington Northern and Santa Fe railroad companies. He completed the work in 1997, after which he began the Delta assignment.

After Feld left *Delta Technology* following the end of the Year 2000 Program, a succession of employees filled the role of CEO:

- Bob DeRodes joined Delta in 1999 and resigned in 2002 to work for Home Depot.
- Curtis Robb moved into the role in an acting position in February 2002, after Bob DeRodes left. Robb was made official CIO of the airline and CEO of the subsidiary in June 2002. He retired on April 1, 2005, and now works for Home Depot.
- Brian Leinbach was named Sr. VP and CIO of Delta Airlines and president and CEO of *Delta Technology* in April 2005. He left late in 2005.
- Shirley Bridges succeeded Leinbach.

Walter Taylor

Taylor served as VP – Air Operations Portfolio, and Director, Year 2000 Program in *Delta Technology* from 1997 - 2000. Immediately following the year 2000 rollover, Taylor was Tech Ops division's CIO. He served as Managing Director of Maintenance,

Repair, and Operation Process and Technology for Tech Ops, then as Managing Director of Finance & Supply Chain Technology and Profit Improvement before his departure from Delta in 2004. In that capacity, he was responsible for the ERP implementation and management using SAP technology to provide Finance and Supply Chain capabilities and was responsible for a revenue enhancement program to begin the process of returning Delta to profitability.

Taylor served for eight years in the U. S. Air Force where he was an officer and pilot. He is a veteran of Desert Storm. He joined Delta as a pilot, and then went to Total Systems (TSYS), the number two credit card processor, for two years as an IT project management consultant. Taylor then spent two years with EDS (where Feld is now employed) in natural gas & transportation before returning to Delta as a pilot and his assignment in *Delta Technology* leadership. Taylor worked for Delta for a total of 8 years.

Wayne Hyde

Delta hired Wayne Hyde, a business intelligence expert, in 1998 to help assemble its data warehouse. Hyde had worked at Frito-Lay and Burlington Northern Santa Fe Railway.

APPENDIX D

DELTA'S Y2K DEPENDENCIES

IT APPLICATION SYSTEMS

Customer Portfolio	Business Support Portfolio
Operations Portfolio	Revenue Portfolio

EQUIPMENT

Aircraft

Simulators & Flight Training Devices

Tools & Diagnostic Equipment

FACILITIES

General Office Complex & Other Owned Facilities

Airports

RES Centers

DSOs

CTOs

Air Cargo

Maintenance Hangar

SUPPLIERS

Fuel Suppliers	Aircraft & Aircraft Parts
Ground Handling	Utility Providers
Alliance Partners	Connection Carriers

REGULATORY AGENCIES

FAA	Customs
DOT	National Weather Service
APHIS	International Air Traffic Services
INS	

INDUSTRY OWNED ORGANIZATIONS

ATA	Airlines Clearing House (ACH)
IATA	Airline Reporting Corporation (ARC)
ATPCO	Aeronautical Radio, Inc. (ARINC)
NAV Canada	Air Cargo Inc. (ACI)

APPENDIX E

DELTA Y2K PROGRAM OVERVIEW FACTS

> Millions of staff hours, dollars, digging and deliberation have gone into making *Y2K* a 'non-event'. At DELTA and in the airline industry we feel confident that aviation will be as safe on January 1, 2000 as it is today. While it may not all run perfectly, we do not anticipate anything more than what would be experienced during a weather operation (Delta archive, "Delta Y2K Program Overview Facts," 1999).

The following information on the status of *Y2K* activities is taken directly from the Delta archive, "Delta Y2K Program Overview Facts," 1999.

Delta Y2K Business Program

- Working closely with ATA, ATAC (ATA Canada), IATA
- Program covers: internal airline assets, airports, suppliers (business and IT areas)
  - Internal airline equipment & assets: IT & Non-IT Equipment (SIMS, aircraft, diagnostic tools, office equipment) ECD June 30
  - Airports: DL metal, Connection carriers, alliances & code-share; ECD June 30
  - Suppliers: categorized by criticality - High, Medium, Low. Concentrating on Highs (the ones who really matter)
- Methodology: Inventory, Assessment, Remediation, Testing, Implementation, Monitoring
- $25M estimated spending for the business program
- Focusing on Business Continuity Plans
- Delta is a sponsor of:
  - Atlanta Year 2000 User Group
  - GA Utilities Forum
  - SBA (aid to/from Small Businesses)
- Managing the Roll Over....Delta will
  - operate as normal
  - staff a *Y2K* Command Center
  - handle any anomalies
  - make *Y2K* a 'non-event'

U.S. Air Transport Association

- ATA/ATAC: joint program ... not a competitive issue, but a cooperative issue
- Contracted Price Waterhouse Coopers (PWC) for airport site visits
- All major airlines participating(107 carriers including Canadian carriers and RAA members)
- $15 million budget
- RAA/Connection carriers were included
- Program focused on:

- Airports: airport workshops/seminars were held to assist airports with initiating *Y2K* programs. Details of this area of the *Y2K* program include obtaining a complete airport system inventory, statusing the systems based on criticality, and tracking *Y2K* readiness
- Suppliers: this portion of the program focuses on the most critical suppliers that airlines share in common (fuel, communications, aircraft and aircraft parts, etc.) Face-to-face meetings were held initially with periodic follow-up.
- Government Entities (NAVCANADA/FAA, APHIS, National Weather Service (NWS), Customs, Immigrations & Naturalizations) and Industry Owned organizations (SITA, AIRINC, ATPCO, etc.): focused on the readiness of government agencies and industry-owned organizations

- Pushing airlines and airports to develop contingency plans
- ATA would have a *Y2K* Command Center set up on 12/31/99
- Working on an extensive communications plan

International Air Transport Association

- Working with regional and global organizations (ICAO, etc.)
- Contracted PWC for airport and ATS site visits
- Over 200 participating airlines
- $19 million budget (plus asking for $6M more)
- RAA/Connection carriers were included
- Program focused on:
  - Airports: airport workshops/seminars were held to assist airports with initiating their *Y2K* programs. Held 26 Awareness Seminars, conducted site visits to 72 airports and sent *Y2K* kits to over 2,500 airports. Details of this area of the *Y2K* program included obtaining a complete airport system inventory, statusing the systems based on criticality, and tracking *Y2K* readiness. Conducted monthly follow-up.
  - ATS/FIRs: visited over 100 sites. Monthly follow-up and some site re-visits
  - Suppliers: Minimal focus as most suppliers were handled under ATA program
  - Government Entities: somewhat engaged with ICAO. Customs was added to the program. 37 of 45 world customs organizations responded.
- Urging airlines and airports to develop Contingency Plans.
- Working on a public communications plan

U.S. Federal Aviation Administration

- Program Director: Ray Long
- Program Methodology: Inventory, Assessment, Remediation, Implementation, Testing
- ECD June 30, 1999 - on target; if not slightly ahead
- FAA reported that of 636 critical and non mission critical systems, 90% were compliant with 89% of the mission critical systems ready. They expect all mission critical systems to be ready by June 30, 1999.
- End:End Testing - Denver - April 1999
  - dual system testing

  - airline involvement - UAL
  - very successful - "blissfully boring" was the comment given; No problems occurred that were related to *Y2K*. Analysis of each software bit showed no deviation from the normal operation.
  - may do further end:end testing, but not necessary as all tests to date have been fine. Delta encouraged ATL Hartsfield to participate in testing with FAA (target timeframe is August)
- FAA focused on OMB's list of 50 systems and believed there would be no service interruption
- As systems became compliant, code audits and configuration management assured their continued integrity.
- Additional testing conducted in host computer systems, air traffic en route centers
- Worked on a public communications plan
- FAA's international focus was on areas that affect 60% of the domestic originated travel:
  - Canada
  - Mexico
  - Bahamas
  - Japan
  - United Kingdom
  - Dominican Republic
- FAA not expected to provide meaningful evaluation of information received on the readiness of other nation-states. The U.S. Department of State was involved there. There was a reluctance to cite a non-U.S. service provider as non-compliant or to say we should not operate to or over a particular state. This was somewhat contradictory to the security cautions regarding certain airports, e.g., Port-a-Prince & Zaire.
- FAA developed contingency plans and requested airline involvement in such areas as ATC, capacity/flow control.
- FAA inspectors made site visits to airlines

NOTE: While FAA has <u>not</u> had access to the detailed information obtained in the ATA database, FAA has worked openly and willingly with ATA and member airlines and built a close working relationship for dealing with *Y2K*

Aircraft manufacturers

- Boeing
  - no safety of flight issues
  - completed ground/flight demonstrations for *Y2K* readiness
  - successfully completed ground and flight demonstrations on all current production models. Absolutely no effects to the flight deck or operation of the aircraft occurred.
  - Boeing expects to complete its internal preparedness activities by July 1999.
  - War room established in SEA
- Airbus
  - no safety of flight issues

- Aircraft Component Manufacturers - similar programs/testing, good results
- Power plant manufacturer representatives from GE and Roll Royce concur with Boeing that there are no *Y2K* engine issues

Delta Air Lines Year 2000 Report to Shareholders

This section is taken directly from Delta's Annual Report (1999, p. 29-31).

YEAR 2000

Our Company has completed all phases of our Year 2000 program for our aircraft fleet, onboard flight support systems, and onboard flight management systems. In addition, all Year 2000 phases for our ground-based, safety-related computer systems and equipment and all critical internal business systems are complete. We will continue to test selected systems and equipment through December 31, 1999 as part of our normal systems maintenance. We will also monitor these systems well into calendar year 2000 to confirm that our hardware and software are operating correctly.

We are replacing customer service hardware that is currently installed at our airport facilities with upgraded, Year 2000 compliant hardware. We began this effort in September 1998 and expect to complete installation during the December 1999 quarter.

We will continue to communicate with third parties during the December 1999 quarter to determine our exposure to the failure of the third parties to remediate their Year 2000 issues, and to resolve any problems discovered to the extent practicable.

Our Company estimates that the total cost of achieving Year 2000 readiness for our internal systems and equipment is approximately $110 million. We have recognized $97 million as expense ($6 million of which was incurred in the September 1999 quarter) in our Consolidated Statements of Operations through September 30, 1999.

This "Year 2000" section is a "Year 2000 Readiness Disclosure" within the meaning of the Year 2000 Information and Readiness Disclosure Act enacted in October 1998. This "Year 2000" section includes forward-looking statements as defined in the Private Securities Litigation Reform Act of 1995. Our Company uses the words "believes", "expects", "estimates" and similar expressions to identify forward-looking statements. Forward-looking statements involve a number of risks and uncertainties that could cause the actual results to differ materially from the projected results. Factors that could cause these differences include, but are not limited to:

- the ability to identify and remediate all date-sensitive lines of computer code or to replace embedded computer chips in affected systems or equipment;
- the availability of qualified personnel and other information technology resources; and
- the actions of governmental agencies or other third parties with respect to Year 2000 problems.

CRITICAL INTERNAL BUSINESS SYSTEMS

Our critical internal business systems and equipment include computer hardware, software and related equipment essential for the following functions:

- customer reservations
- ticketing
- flight scheduling
- seat inventory management
- airport customer services
- finance administration
- internal voice and data communications
- aircraft ground handling
- baggage handling
- facility management
- security

We have completed the identification and assessment phases for all of our critical internal business systems and equipment. Remediation is in process for one of our vendor-supported baggage handling systems, and we expect to complete its remediation and testing by October 1999. We have completed the remediation and testing phases for all other critical internal business systems and equipment. We will continue selective testing of our critical internal business systems through December 31, 1999 as part of normal systems maintenance. We will monitor remediated and tested systems well into calendar year 2000 to confirm that our hardware and software operates correctly.

We are replacing customer service hardware that is currently installed at our airport facilities with upgraded, Year 2000 compliant hardware. We began this effort in September 1998 and expect to complete installation during the December 1999 quarter.

INTERFACES WITH THIRD PARTIES

Our Company has communicated with, and continues to review, third parties that provide essential goods or services to our Company in order to:

1. determine the extent to which we are vulnerable to the failure of these third parties to remediate their Year 2000 issues, and

2. resolve any problems discovered to the extent practicable.

These third parties include suppliers of infrastructure critical to the airline industry, such as air traffic control and related systems of the U.S. Federal Aviation Administration and international aviation authorities, the U.S. Department of Transportation (DOT) and local airport authorities. Other critical third parties include other airlines as well as suppliers of aircraft fuel, utilities, external computer reservations services and communication services. We are actively involved in airline industry Year 2000 review efforts led by the

Air Transport Association (ATA), the International Civil Aviation Organization (ICAO) and the International Air Transport Association (IATA). This review has identified potential Year 2000 compliance issues at several international locations. Delta, along with other airlines and the ATA, ICAO and IATA, is continuing to assess these specific situations. We will make future flight schedule revisions if necessary to ensure safe operations.

ESTIMATED YEAR 2000 COSTS

Our Company estimates the total cost of achieving Year 2000 readiness for our internal systems and equipment is approximately $105 million to $120 million, of which $91 million has been recognized as expense in the Consolidated Statements of Operations through June 30, 1999. The majority of the estimated Year 2000 compliance costs have been funded by reallocating existing resources rather than incurring incremental costs.

CONTINGENCY PLANNING

We revised our existing business interruption contingency plans to address internal and external issues specific to the Year 2000 problem. These plans are intended to enable us to continue to operate, to the extent that we can do so safely. Our contingency plans include performing processes manually, repairing or obtaining replacement systems, changing suppliers and reducing or suspending operations.

We believe, however, that due to the widespread nature of potential Year 2000 issues, the contingency planning process is ongoing and will require further modifications as we receive information about the results of the Year 2000 programs of Delta and of third parties.

POSSIBLE CONSEQUENCES OF YEAR 2000 PROBLEMS

Management believes that completed and planned modifications and conversions of our Company's internal systems and equipment will allow us to be Year 2000 compliant in a timely manner. There can be no assurance, however, that our internal systems or equipment or those of the third parties on whom we rely will be Year 2000 compliant in a timely manner, or that our Company's or third parties' contingency plans will mitigate the effects of issues that arise. The failure of our systems or equipment or of an essential third party (whose failure we believe is the most reasonably likely worst-case scenario) could result in the reduction or suspension of our operations and could have a material adverse effect on our business or consolidated financial statements.

OTHER MATTERS

The section above entitled “Year 2000 Readiness” is a “Year 2000 Readiness Disclosure” within the meaning of the Year 2000 Information and Readiness Disclosure Act (Public Law 105-271) enacted in October 1998.

APPENDIX F
TEMPLATE FOR STANDARDIZING DESKTOP UNITS

COMPUTING MODEL ATTRIBUTES
Identification • Portfolio ID (PORTFOLIO: Portfolio_Id) • Portfolio Name (PORTFOLIO: Portfolio_Nm) • Division (A25) • Computing Model Name (A25) • DAL -Owner (A25) • *Delta Technology* Owner (A25) • Renewal Owner (A15) • Priority • Y2k Impact • Number of Installations (n5) • Locations (A50)
Delta Applications • Application Name (A25) • Application Description (A50) • Application Owner (A25) • Owner Phone (A8) • Compiler (Use SFTWR_TYP & SOFTWARE tables to list products identified as “Language”) • Database (Use SFTWR_TYP & SOFTWARE tables to list products identified as “DBMS”)
***Delta Technology* Applications** • Application ID (APPLICATION: NUMBER) • Application Name (APPLICATION: Sys_Nm)
Work Group Products • COTS Product Name (Use SFTWR_TYP & SOFTWARE tables to list products identified as “Business Application”)
Operating System • COTS Product Name (Use SFTWR_TYP & SOFTWARE tables to list products identified as “Computer Operating System”)
Desktop Hardware • COTS Product Name

Source: Delta archive, Computing Model.doc, 1998.

APPENDIX G

OPERATIONAL DEFINITIONS FOR STUDY VARIABLES

Systems

Groups of related software at Delta

Y2K solutions

Changes to systems in a business area over the period 1997-2003

Business area

A collection of sub-unit divisions of Delta categorized by its relationship to one of the four core business functions: *Business Support*, *Airport Customer Service*, *Operations*, and *Revenue*

Business area characteristics

- Size – measured as number of employees and/or functional divisions
- Activities – measured by roles and functional divisions
- Number of system users - measured by number of desktop units
- Organization complexity – measured by relative size, number of geographic locations, variety of activities and specialized occupations, number of systems (home grown and/or COTS, mission critical, number of interfaces) and system users, evidence of organization adaptation: the complexity of environments as reflected in the complexity of the business area.
- Cultural character – measured by evidence of cultural concepts (Delta family, military or union, and perception of information security or safety)
- Regulatory environment – government and industry affiliations
- Time constraint – measured by observations related to history of systems and estimated completion date (ECD) for *Y2K* compliance

Institutionalized environment

Evidence of structural systems that had become established over time in Delta's environment, i.e., "federations, associations, customer-supplier relationships, competitive relationships, and a social-legal apparatus defining and controlling the nature and limits of relationships" (Pfeffer & Salancik, 1978)

Nature of the *Y2K solution*

Institutional model

An institutional model demonstrates a departure from rational process and / or decision-making, and often demonstrates unanticipated results. Note that institutional model performance can provide strategic benefits.

Evidence of institutional process

- Regulative: required for maintaining organizational legitimacy
- Cultural:
  - Social fact: perceptions of information technology, information security, safety and other values
  - Familiarity (easy to keep doing what is familiar without evaluating)
  - History with a system (accustomed to using/maintaining)
  - Established relationship (Upgrade to latest model from known vendor. Quick fix for existing, and outdated system already in Delta production, effect of time constraint)

Evidence of institutional decision-making

- Mimetic (effect of complexity and time constraint)
  - Fashionable, bandwagon effect

    Strategic benefits[7]

    Likely to find computer professionals that are familiar with the product

    Likely to get support or interconnect with external users

    Readily available (quick to implement, vendors ready to accommodate)
  - Recommended by consultant

    Strategic benefits

    Product endorsement related to competence in specialized skills

    Opportunity for outside resources
  - Previously applied at sites outside organizational boundaries

    Strategic benefit

    Evidence that product has been installed

    Opportunity to get feedback from users
  - Added pizzazz that presented an up-to-date image

    Strategic benefit

    Customers attracted to look & feel of innovation

    Mechanism for differentiation from competition

[7] Including strategic benefits under the headings of institutional mechanisms is designed to show the difficulty in completely isolating institutional factors.

Rational-contingency model

A rational-contingency model demonstrates a (more or less) efficient and/or effective form of organization. Rational-contingency mechanisms are related to organization of labor, goal orientation, reducing complexity, increasing predictability and the resulting effects on efficiency of operation, including productivity, cost reductions, and revenue increases.

Evidence of rational process

- Goal orientation
- Communications related to mission control

Evidence of rational decision-making

Decision criteria for *Y2K solution* (best solution)

- Understanding of system criticality
- Tests for *Y2K* compliance
- Fit with functional activities
- Reduces complexity
- Improves predictability
- Highest efficiency related to cost, processing, resources, etc.
- A specialized, well-functioning in-house system (no immediate replacement option, inadequate current resources to re-write)
- A secure system (reasonably up-to-date, well-documented, easily supported, produces output as designed, etc.)

Information security

The state of a computer-based system whereby electronically stored and / or transmitted information is adequately protected. Adequate protection relates to assurance of the confidentiality, integrity, availability, accessibility (including appropriate mechanisms for authorization), and non-repudiation of information.

Information security management

Evidence related to means (technical and non-technical) for maintaining information security

APPENDIX H

ENVIRONMENTAL FACTORS

RELATED TO *Y2K SOLUTION* IN DELTA BUSINESS AREAS

Table 72: Environmental factors related to business area responses

OPERATIONAL DEFINITIONS	**FACTORS:** RELATED TO BUSINESS AREA RESPONSE TO THE *Y2K* CONTINGENCY (i.e., *Y2K Solution*)
Institutional model	(Contingency: *Y2K bug*)
CATEGORIES OF EVIDENCE RELATING TO AN INSTITUTIONAL PROCESS	FACTORS THAT CONTRIBUTE TO AN INSTITUTIONAL PROCESS
Cultural • Related to a social fact: perceptions of air transportation, information technology, information security, safety or other value • Cognitive, e.g., military culture • Familiar, comfortable, habitual, e.g., family culture • Related to established relationships, e.g., ALPA, vendors, consultants	16. Organizational leadership: • Inaction, not taking Y2K or information security seriously o Lacking vision or understanding o e.g., Delta investing in OCC etc. when *Y2K* had not been investigated 17. Condition of business area and its IT systems: • Systems working but without documentation • IT employees inadequately trained internally and hired for life • IT employees content with the status quo • Habit of avoiding outside consultants 18. Character of business area environment: • Inadequate condition in industry organizations' IT systems • Standards and regulations focused on a limited view of safety 19. Distraction of other business area contingencies: • Financial status • Economic conditions • War efforts • Pilots' activities • Low cost carriers
CATEGORIES OF EVIDENCE RELATING TO INSTITUTIONAL DECISION-MAKING	FACTORS RELATING TO INSTITUTIONAL DECISION-MAKING IN RESPONSE TO *Y2K*
Regulative • Requirements for maintaining organizational legitimacy Mimetic (Following the crowd) • Fashionable, popular • Recommended by consultant • Previously applied at sites outside organizational boundaries	20. U.S. laws, industry regulations: • SEC & legislature were the only regulators that put any level of teeth into *Y2K* compliance, but it was minimalist. Even at the last, a loophole was created to relieve companies of liability. • Industry regulations were focused on safety of air transportation, but not linked to information security. 10. Character of business area environment: • Chaos because of time limitation • Scarcity of personnel resources • Availability of IT products in the marketplace

Table 72 continued

OPERATIONAL DEFINITIONS	**FACTORS:** RELATED TO BUSINESS AREA RESPONSE TO THE *Y2K* CONTINGENCY (i.e., *Y2K Solution*)
Rational-contingency model	
CATEGORIES OF EVIDENCE RELATING TO A RATIONAL PROCESS	FACTORS THAT CONTRIBUTE TO A RATIONAL PROCESS IN IT MANAGEMENT
Goal orientation Evidence of decreasing complexity, improving predictability Actions relating to efficiency and effectiveness Communications related to mission control	11. Organizational leadership: • Acts in advance of crisis, investigate, inventory • IT Dept. alerts execs to needs for resources, etc. • Desires to make enterprise more competitive 12. Condition of business area and its IT systems: • Process in place that assures continual assessment with respect to condition of systems and efficiency of performance; e.g., in processes of reengineering, have employees and/or consultants assist in maintaining systems inventory / assessment. • Process in place that considers the possibility for achieving greater efficiency 13. Character of the business area environment: • Government and industry organizations stay current with safety *and* security of their own systems 14. Responses to business area contingencies: • Management of budget, financial condition • Anticipating change in economic conditions, community & military needs, pilot demands • Competitive market changes
CATEGORIES OF EVIDENCE RELATING TO RATIONAL DECISION-MAKING	FACTORS RELATING TO RATIONAL DECISION-MAKING IN RESPONSE TO *Y2K*
Regulative Requirements for maintaining organizational effectiveness Decision-making criteria • Based on knowledge of systems o Y2K compliance o Fit with functional area o Efficiency related to cost, processing, resources, etc. o Systems & information security	11. U.S. laws, industry regulations: • A bounding framework of rules wherein the condition of IT systems is recognized as vital to safety and national security 12. Organizational leadership: • Knowledgeable about information technology and information security • Values the contribution of IT to the functioning of the organization • Employs personnel with high levels of skills • Applies incentive systems to maintaining employee skills and levels of professional certification • Adequately develops and maintains IT systems • Adequately responds to security contingencies 9. Character of business area environment: • Personnel resources available • Appropriate and adequate IT products in the marketplace

APPENDIX I

DELTA YEAR 2000 ARCHIVE

This dissertation is based on many hours of interviews, as well as thousands of pages of published and unpublished materials. The archive of the Delta Year 2000 Program (Delta archive) was the principal source for unpublished materials. This section provides a reference list for these proprietary and confidential Delta Air Lines documents that were cited in the body of the dissertation. The Delta archive had no uniform format for documents; therefore, the documents are described by electronic file name, and/or according to identifying information that appeared on the documents themselves. Most of the documents were stored on CD-ROM, and were located in a directory named CMLibrary1. Those that were provided as hard copy (with no backup to electronic media) are noted in the reference entry.

TERMINOLOGY AND DEFINITIONS

Page

xxiii. Asset Compliance Management Plan. (1998, Feb. 28). ACMPLAN.doc.

xxvii. dt147. (hard copy only).

xxix. Y2K CM Delta Divisions.doc

xxxi. Delta Technology, Inc. Statement of Work: Version 3.1 (1998, Mar 13). Y2K Engineering SOW.doc.

xxxv. Workshop Presentation.ppt.

xxxvii. Definiti.doc

CHAPTER 1: HOUSTON, WE'VE HAD A PROBLEM

Page

10. Mission Year 2000 Master Plan, Section 1.0 Executive Summary. (1998, Feb).

CHAPTER 3: SETTING UP THE INVESTIGATION

Page

80. Delta Year 2000 Program Briefing Book. (1999, Feb).

CHAPTER 5: THE CASE OF DELTA AIR LINES: ITS CRITICAL INFRASTRUCTURE

Page

125. Year 2000 Program Briefing Book. (1999, May 21).

132. (1998). 061298.txt.

CHAPTER 6: THE YEAR 2000 PROGRAM SUPPORTED DELTA'S FUTURE VISION

Page

134. Mission Year 2000 Master Plan, Section 1.0 Executive Summary. (1998, Feb).

Delta Air Lines IT Costs (McCullough letter). ITCosts.doc.

Taylor, W. (2000). Corporate Communications. Y2K-Normal.doc.

139. Figure 3-3. Mapping Technical and Business Risks. (1997, Dec 31). SEC_Definitions.doc.

140. Delta's Enterprise Year 2000 Management Overview Inventory Phase. (1997, Nov 11). INVOV2_0.doc.

141. Res Conference.ppt.

145. Year 2000 correspondence E-GDTS-1606-006.00.

. EC Update0399.ppt.

146. Workshop Presentation.ppt.

(1997, Dec). ASR_123197 Lang-LOC stats 12.97.doc.

147. (1998, Apr). OPS Migration plan 04.98.ppt.

(1999). ACT_ITMS.xls.

152. (1997, Dec). ASR_123197 Lang-LOC stats 12.97.doc.

153. (1998, Apr). OPS Migration Plan 04.98.ppt.

157. (1998). Y2K Desktop Charter.

158. BA Review.doc.

159. Y2K Desktop charter.doc

161. Y2K-Normal.doc.

BODDec97.doc.

Y2K Program Overview Facts.doc.

161. BODMar98.doc.

163. ACT_ITMS.xls, 1999.

164 EC Update0399.ppt.

BODDec97.doc.

165. ACT_ITMS.xls, 1999

Year 2000 Program Briefing Book. (1999, May 21).

CHAPTER 7: PROGRAM ROLLOUT TO DELTA'S SUB-UNIT BUSINESS AREAS

Page

177. Metrics.xls.

180. Assessment Summary Report of Dec 31, 1997. (1997, Dec 31).

(1999, Mar). Customer Summary Document.doc.

183. Defnote1.doc.

193. dt43. (1998, Apr), hard copy only.

203. email. (2005).

208. (1999). Act_Itms.xls.

Year 2000 Program Briefing Book. (1999, May 21).

209. (1999). Act_Itms.xls.

234. Defnote1.doc

CHAPTER 9: WHAT HAPPENED TO INFORMATION SECURITY?

Page

278. Taylor, W. (2000). Y2K-Normal.doc.

282. Sec 1.

288. Year 2000 Hardware Assessment, Impact Analysis and Renovation Project Plan Version 1.0. (1998).

290. (1999, Apr 21). COTS state of the union.doc.

CHAPTER 10: CONCLUDING COMMENTS

Page

309. Delta Year 2000 Program Briefing Book. (1999, May 21). Delta Year 2000 Program Briefing Book.doc.

APPENDIX F: DELTA Y2K PROGRAM OVERVIEW FACTS

Page

346. Delta Y2K Program Overview Facts. (1999, May 6). Delta Y2K Program Overview Facts.doc.

APPENDIX G: TEMPLATE FOR STANDARDIZING DESKTOP UNITS

Page

352. (1998, Oct 12). Computing Model.doc.

REFERENCES

A History of Service. (2003). Delta Air Transport Heritage Museum, Inc. Retrieved May 2007, from http://www.deltamuseum.org/M_Education_DeltaHistory_Facts_History.htm.

Abbate, J. (1999). *Inventing the Internet*. Cambridge, MA and London: MIT Press.

Abell, P. (1995). The New Institutionalism and Rational Choice Theory. In W. R. Scott & S. Christensen (Eds.), *The Institutional Construction of Organizations.* Thousand Oaks, CA: Sage Publications.

Allison, G. T., & Zelikow, P. (1999). *Essence of Decision: Explaining the Cuban Missile Crisis* (2nd ed.). New York: Longman.

Allison, R. (2003, Oct). Hacker attack left port in chaos. Retrieved Oct 2004, from http://www.guardian.co.uk/online/news/0,12597,1057454,00.html

American Bar Association (ABA), Section of Science & Technology Law, Privacy & Computer Crime Committee. (2003). *International Corporate Privacy Handbook*.

Anderson, R. J. (1994). Why Cryptosystems Fail. *Communications of the ACM*, 37(11), 32-40.

_____. (2001a). Why Information Security is Hard - An Economic Perspective. Paper presented at the Computer Security Applications Conference, New Orleans, Louisiana.

_____. (2001b). *Security Engineering: A Guide to Building Dependable Distributed Systems*: John Wiley & Sons, Inc.

Anthes, G. (2004, May 10). Managing IT risks at Delta: The airline uses a rigorous but simple scorecard to balance the risk of technology failure against the costs of upgrading. Retrieved Apr 2007, from http://www.computerworld.com/managementtopics/management/story/0,10801,92931,00.html.

Arndt, M., & Bigelow, B. (2000). Presenting Structural Innovation in an Institutional Environment: Hospitals' Use of Impression Management. *Administrative Science Quarterly, 45*(3), 494-523.

Astley, W. G., & Van de Ven, A. H. (1983). Central Perspectives and Debates in Organization Theory. *Administrative Science Quarterly*, 28, 245-273.

At Hartsfield International Airport, one of the world's busiest, billing records are kept by hand. (1997, Oct 3). Retrieved Apr 2005, from http://ajc.com.

Babington, C. (2007, Mar 5). Daylight Saving Computer Challenges. Retrieved Mar 2007, from http://www.washingtonpost.com/wp-dyn/content/discussion/2007/03/02/DI2007030200946.html.

Barlas, S. (1999). Congress seeks Y2K shield. *Strategic Finance, 80*(11).

Barton, P. (1998, Aug 28). FAA gets main blame for Comair crash: Comair pilots didn't receive icing information. Retrieved Apr 2007, from http://www.enquirer.com/editions/1998/08/28/loc_comair28.html

Beach, G. (2000, Jan 27). The Year 2000 Computer Problem. Prepared testimony before the House Science Committee Subcommittee on Technology, and the House Government Reform Committee Subcommittee on Government Management, Information and Technology.

Becerra-Fernandez, I., & Sabherwal, R. (2001). Organization Knowledge Management: A Contingency Perspective. *Journal of Management Information Systems*, 18(1), 23-55.

Bennett, A., & George, A. (1998). An Alliance of Statistical and Case Study Methods: Research on the Interdemocratic Peace. *APSA-CP Newsletter*, 9(1), 6-9.

Berlind, D. (2003, Oct 22). Ex-cybersecurity Czar Clarke Issues Gloomy Report Card. Retrieved Nov 2003, from http://techupdate.zdnet.com/Clarke_issues_gloomy_report_card__print.html.

Bigelow, R. (1995). Legal Issues in Computer Security. In A. E. Hutt, et al (Ed.), *Computer Security Handbook* (3rd ed.). New York: John Wiley & Sons, Inc.

Bitran, G. R., Gurumurthio, S., & Sam, S. L. (2006). Emerging Trends in Supply Chain Governance. Retrieved Jul 2006, from http://mitsloan.mit.edu/pdf/ups.pdf.

Brown, P. (2003). Getting Inventories In Order: Limited cash is making aviation companies more creative in their inventory management solutions. *Overhaul & Maintenance, IX*(3), 32.

Brush, C. (2001, Jul). Surcharge for Insecurity. Retrieved Sep 2004, from http://www.infosecuritymag.com/articles/july01/departments_news.shtml.

Byers, S., Rubin, A. D., & Kormann, D. (2003). Defending Against an Internet-based Attack on the Physical World. Retrieved Sep 2004, from http://www.avirubin.com/scripted.attacks.pdf.

Caldwell, B. (1997). Delta Powers Up: Airline's control center uses object technology to move 2,700 flights a day. *InformationWeek* (613), 85-88.

Camic, C., & Gross, N. (1998). Contemporary Developments in Sociological Theory: Current Projects and Conditions of Possibility. *Annual Review of Sociology, 24*, 453-476.

Cannon, A. R., & Woszynski, A. B. (2002). Crises and Revolutions in Information Technology: Lessons Learned from Y2K. *Industrial Management & Data Systems, 102*(6), 318-324.

Carr, D. F., & Cone, E. (2002, Apr 8). Can FAA Salvage Its IT Disaster? Retrieved May 2007, from http://www.baselinemag.com/article2/0,1397,818797,00.asp.

Cason, R. (2002, Feb 11). Flight attendants reject union representation. *Delta NewsDigest, 9,* 12.

Chandler, J. G. (2003, Dec 4). How far we have come. Retrieved Apr 2007, from http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=om&id=news/om1203chd.xml.

Charles, J. (2005, Jan 4). Tribe Shoots Arrows at Aid Flight. Retrieved May 2005, from http://news.bbc.co.uk/2/hi/south_asia/4144405.stm.

Chestnut, J. A. (2000). Assessing the Impact of Human Error in Information Security Incidents. Unpublished Ph.D., Mississippi State University.

Cohen, F. (1998). Managing Network Security: The Real *Y2K* Issue. *Network Security* (11), 8-11.

Cohen, L. R., & Noll, R. G. (1991). *The Technology Pork Barrel*. Washington D.C.: Brookings Institution Press.

Cohen, M. D., March, J. G., & Olsen, J. P. (1972). A Garbage Can Model of Organizational Choice. *Administrative Science Quarterly*, 17(1), 1-25.

Collier, D. (1998). Comparative Method in the 1990s: Introduction. *APSA-CP, 9*(1), 1-5.

Committee on National Security Systems (CNSS). (1999, Jul). The Insider Threat to U.S. Government Information Systems. Retrieved Apr 2004, from http://www.nstissc.gov/Assets/pdf/NSTISSAM_INFOSEC1-99.pdf.

Corcoran, E. (2000, Jul 24). The E-Gang: Leo Mullin Embrace the Threat. *Forbes Magazine* Retrieved Nov 2006, from http://www.forbes.com/forbes/2000/0724/145_01.html.

Corporate compliance is everyone's responsibility. (1997, Jan 10). *Delta NewsDigest, 4,* 10.

Creswell, J. W. (2003). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (2nd ed.). Thousand Oaks, CA: Sage Publications.

Curley, M. (2004). The Delta Technology Operating Tail. In *Managing Information Technology for Business Value* (Appendix A). Hillsborough, OR: Intel Press.

Dalton, G. W., Lawrence, P. R., & Lorsch, J. W. (Eds.). (1970). *Organizational Structure and Design*. Homewood, IL: Richard D. Irwin, Inc. and The Dorsey Press.

Davis, R. (2000, May 30). 'Byte' of the love bug shows need for vigilance. *Delta NewsDigest, 7,* 12.

_____. (2001, Mar 5). Delta's anti-virus team gets proactive. *Delta NewsDigest, 8,* 11.

DEC puts airline maintenance reports on-line at Delta. (1991). *Digital Review,* 8(17), 1.

Deck, S. & Stedman, C. (1999, Feb 22). Delta/Baan venture among largest in sales automation. Retrieved Apr 2006, from http://www.computerworld.com/1999/0,4814,34100,00.html.

de Jager, P. (1993, Sep). Doomsday 2000. *Computerworld, 27,* 105-109.

Delta Air Lines. (1997). *1997 Annual Report*. Atlanta: Delta Air Lines.

_____. (1998). *1998 Annual Report*. Atlanta: Delta Air Lines.

_____. (1999) *1999 Annual Report.* Atlanta: Delta Air Lines:

_____. (1999, Sep). *10-Q*. Atlanta: Delta Air Lines.

_____. (2000). *2000 Annual Report*. Atlanta: Delta Air Lines.

_____. (2001, Aug). *8-K*. Atlanta: Delta Air Lines.

_____. (2003). *2003 Annual Report*. Atlanta: Delta Air Lines.

_____. (2004). *2004 Annual Report*. Atlanta: Delta Air Lines.

_____. (2006). Continuity of Business Glossary. Unpublished listing of terminology used in *Delta Technology* (proprietary information). Atlanta: Delta Air Lines.

Delta Air Lines installs new route planning system. (2000, Nov 28). Retrieved Jun 2007, from http://www.taborcommunications.com/dsstar/00/1128/102438.html.

Delta stays mum on cause of IT glitch. (2004, May 10). *Computerworld Magazine*, 8.

Delta taps Jacada for scheduling. (2000, Jul 31). *InfoWorld*, 22, 40.

Delta Technology Fun Facts. (2003). Delta Technology corporate brochure, rev 040804. Atlanta, GA.

Denning, D. E. (1997). Digital Communication Must Not Weaken Law Enforcement. In M. D. Ermann, M. B. Williams & M. S. Shauf (Eds.), *Computers, Ethics, and Society* (2nd ed.). New York and Oxford: Oxford University Press.

Dery, D. (1984). *Problem Definition in Policy Analysis*. Lawrence, KS: University Press of Kansas.

Dhillon, G. (Ed.). (2001). *Information Security Management: Global Challenges In the New Millennium*. Hershey, PA: Idea Group Publishing.

Dhillon, G., & Backhouse, J. (2001). Current Directions in IS Security Research: Towards Socio-Organizational Perspectives. *Information Systems Journal*, 11(2), 127-153.

DiCarlo, L. (2004, Apr 20). The Revolving Door on the Flight Deck. Retrieved Apr 2007, from http://www.forbes.com/work/2004/04/20/cx_ld_0420ceos.html.

DiMaggio, P. J. (1988). Interest and Agency in Institutional Theory. In L. G. Zucker (Ed.), *Institutional Patterns and Organizations: Culture and Environment* (pp. 3-21). Cambridge, MA: Ballinger.

DiMaggio, P. J., & Powell, W. W. (1983). The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields. *American Sociological Review*, 48(2), 147-160.

_____. (1991). Introduction. In W. W. Powell & P. J. DiMaggio (Eds.), *The New Institutionalism in Organizational Analysis* (pp. 1-38). Chicago and London: The University of Chicago Press.

Donaldson, L. (1996). The Normal Science of Structural Contingency Theory. In S. R. Clegg, C. Hardy & W. R. Nord (Eds.), *Handbook of Organisation Studies*. London: Sage Publications.

_____. (2001). *The Contingency Theory of Organizations*. Thousand Oaks, CA: Sage Publications.

Donoghue, J. A. (2002). Getting IT Wired. *Air Transport World,* 39(4), 24-26.

Doyle, T., & Gillies, A. T. (2007, Feb 26). Smarter Skies. Retrieved Feb 2007, from http://www.forbes.com.

Drazin, R., and Andrew H. Van de Ven. (1985). Alternative Forms of Fit in Contingency Theory. *Administrative Science Quarterly*, 30, 514-531.

Durkheim, E. ([1901] 1950). *The Rules of Sociological Method*. Glencoe, IL: Free Press.

Dutta, A., & McCrohan, K. (2002). Management's Role in Information Security in a Cyber Economy. *California Management Review*, 45(1).

Eskow, D. (1990). Delta's development plan puts users in charge. *PC Week, 7*(24), 1.

Ezell, B. (1998). Risks of Cyber Attack to Supervisory Control and Data Acquisition for Water Supply. Unpublished Master of Science (Systems Engineering), University of Virginia, Charlottesville.

Feld, C. S., & Stoddard, D. B. (2004). Getting IT Right. *Harvard Business Review* (Feb), 72-79.

Ferraro, F., Pfeffer, J., & Sutton, R. I. (2005). Economic language and assumptions: How theory can become self-fulfilling. *Academy of Management Review, 30*(1), 8-25.

Fligstein, N. (1991). The Structural Transformation of American Industry: An Institutional Account of the Causes of Diversification in the Largest Firms, 1919-1979. In W. W. Powell & P. J. DiMaggio (Eds.), *The New Institutionalism in Organizational Analysis*. Chicago: The University of Chicago Press.

Gage, D., & McCormick, J. (2003, Apr 1). Delta's Last Stand. *Baseline: The Project Management Center.* Retrieved Mar 2006, from http://www.baselinemag.com/print_article2/0,1217,a=39941,00.asp.

Galaskiewicz, J., & Wasserman, S. (1989). Mimetic Processes within an Interorganizational Field: An Empirical Test. *Administrative Science Quarterly, 34*, 454-479.

Galbraith, J. (1973). *Designing Complex Organizations*. Reading, MA: Addison Wesley.

Gale, J. R. (1968). Why Management Information Systems Fail. *Financial Executive*, 44-48.

Gallagher, J. D. (1961). *Management Information Systems and the Computer***.** New York: American Management Association.

Garvey, J. (2002, Jul 23). Remarks to The Aero Club, Washington, D.C.

Geography and the Net: Putting It In Its Place. (2001, Aug 9). *The Economist*.

Georgiou, P. (1973). The Goal Paradigm and Notes towards a Counter Paradigm. *Administrative Science Quarterly*, 18(3), 291-310.

Glossary of Key Information Security Terms. (2006, Apr 26). Retrieved May 2007, from http://csrc.nist.gov/publications/nistir/NISTIR-7298_Glossary_Key_Infor_Security_Terms.pdf.

Goodman, S. E. (2001). Chapter 3: The Civil Aviation Analogy, Part I: International Cooperation to Protect Civil Aviation against Cyber Crime and Terrorism. In A. D. Sofaer & S. E. Goodman (Eds.), *The Transnational Dimension of Cyber Crime and Terrorism* (pp.69-72). Stanford, CA: Hoover Institution Press.

_____. (2001, Sep). *The Protection and Defense of Critical Information Infrastructures.* Paper presented at the IISS 43rd Annual Conference, Geneva.

Goodman, S. E., Hassebroek, P. B., King, D., & Ozment, A. (2002, May 20-22). International Coordination to Increase the Security of Critical Network Infrastructures. ITU New Initiatives Workshop: Creating Trust in Critical Network Infrastructures. Retrieved Aug 2004, from http://www.itu.int/osg/spu/ni/security/index.html, http://www.itu.int/osg/ni/security/docs/cni.04.pdf.

_____. (2003). International Coordination to Increase the Security of Critical Network Infrastructures. *Journal of Information Warfare*, 2(2), 72-87.

Goodman, S. E., Hassebroek, P. B., & Klein, H. K. (2003). Visions of the Information Society: Network Security. Retrieved Jan 2005, from http://www.itu.int/osg/spu/visions/networksecurity/paper3.html.

Greening, D. W., and Barbara Gray. (1994). Testing a model of organizational response to social and political issues. *Academy of Management Journal, 37*(3), 467-498.

Greenwood, R., & Hinings, C. R. (1996). Understanding Radical Organizational Change: Bringing Together the Old and the New Institutionalism. *Academy of Management Review*, 21(4), 1022-1054.

Greising, D. (1995, Dec 11). It Hurts So Good at Delta. Retrieved Mar 2007, from http://www.businessweek.com/archives/1995/b345499.arc.htm?chan=search.

_____. (1997, Dec 22). A Break in the Clouds for Delta. Retrieved May 2007, from http://businessweek.com/archives/1997/b3558136.arc.htm.

Gresov, C. (1989). Exploring Fit and Misfit with Multiple Contingencies. *Administrative Science Quarterly*, 34, 431-452.

Gross, G. (2003, Jul). Cybersecurity Laws Expected: Congress Considers Imposing Security Standards On Businesses. Retrieved Sep 2004, from http://www.pcworld.com/news/article/0,aid,111535,00.asp.

Gulick, L. H., & Urwick, L. F. (Eds.). ([1937] 1954). *Papers on the science of administration*. New York Institute of Public Administration, Columbia University.

Gupta, P. P., Dirsmith, M. W., & Fogarty, T. J. (1994). Coordination and Control in a Government Agency: Contingency and Institutional Theory Perspectives on GAO Audits. *Administrative Science Quarterly*, 39(2), 264-285.

Hall, R. H. (1996). *Organizations: Structures, Processes, and Outcomes* (6th ed.). Englewood Cliffs, N.J.: Prentice Hall.

Hamilton, J. S. (2001). *Practical Aviation Law* (3rd ed.). Ames, Iowa: Iowa State Press.

Hannan, M. T., & Freeman, J. (1993). *Organizational Ecology*: Harvard University Press.

Harding, E. U. (1999, Jun). Friendlier Airports: The Goal of Delta's Top Technology Project. Retrieved May 2007, from http://findarticles.com/p/articles/mi_mOSMG/is_1_19?ai_58379507.

Harrington, S. J. (1995). Computer crime & abuse by IS employees. *Journal of Systems Management*, 46(2).

_____. (1996). The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions. *MIS Quarterly*, 20(3), 257-279.

Harris, R. (1997, Dec 1) In-flight Infight. Retrieved May 2007, from http://www.cfo.com/article.cfm/2990648/C_3046568.

Hartsfield City Limits: A $9.3 billion a year impact. (1998, Nov 2). *The Atlanta Journal and the Atlanta Constitution,* p. E3.

Havenstein, H. (2006, Dec 11). Delta set to launch three-year SOA project. Retrieved Apr 2007, from http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=276387.

Hirsch, P. M., & Lounsbury, M. (1997). Ending the Family Quarrel: Toward a Reconciliation of "Old" and "New" Institutionalisms. *American Behavioral Scientist*, 40(4), 406-418.

Hitchings, J. (1995). Deficiencies of the Traditional Approach to Information Security and the Requirements for a New Methodology. *Computers & Security*, 14(5), 377-383.

Hoag, B., & Cooper, C. L. (2006). *Managing Value-based Organizations: It's Not What You Think*: Edward Elgar Publishing, Inc.

Hsu, M.-H., & Kuo, F.-Y. (2003). The Effect of Organization-Based Self-Esteem and Deindividuation in Protecting Personal Information Privacy. *Journal of Business Ethics*, 42, 305-320.

Huitt, W. G. (1999, Jan). Threats to External and Internal Validity. Retrieved Mar 2007, from http://chiron.valdosta.edu/whuitt/col/intro/valddv.html.

International Federation of Air Line Pilots' Associations (IFALPA). (2005, Jan 6). Jargon Buster: Glossary of aviation acronyms, terms and definitions. Retrieved May 2007, from http://www.ifalpa.org/HotNews/03DIR001JargonBuster.pdf.

James, H. L. (1996). Managing Information Systems Security: A Soft Approach. Paper presented at the Information Systems Conference of New Zealand, Palmerston North, New Zealand.

Jensen, D. (2000, Jan 1). Airlines as Jugglers. *Avionics Magazine*.

Jones, G. (2003). *Delta Air Lines: 75 Years of Airline Excellence*. Charleston, SC: Arcadia Publishing.

Ker, N. (1994) Small is beautiful. *The Computer Bulletin*. 6(2) 5-6.

Kingsley, G. "Re: 10 page research project overview attached," E-mail to the author, 2005.

Klein, H. K. (2000). System Development in the Federal Government: How Technology Influences Outcomes. *Policy Studies Journal*, 28(2), 313-328.

_____. (2002). ICANN and Internet Governance: Leveraging Technical Coordination to Realize Global Public Policy. *The Information Society*, 18, 193-207.

Knorr, E. (2004, May 10). Opening up the mainframe. Retrieved Jun 2006, from http://www.computerworld.com.au/index.php?id=651073728&fp=16&fpid=0.

Konicki, S. (2002, Jun 10). Chain Reaction: ERP vendors gain grip on supply-chain software market with convenience on their side. Retrieved Oct 2006, from http://www.informationweek.com/story/IWK20020609S0001.

Lawrence, P. R., & Lorsch, J. W. (1967). *Organization and Environment: Managing Differentiation and Integration.* Boston, MA: Harvard Business School Press.

Leonard, L. N. K., & Cronan, T. P. (2001). Illegal, Inappropriate, and Unethical Behavior in an Information Technology Context: A Study to Explain Influences. *Journal of the Association for Information Systems, 1*(12).

Lessig, L. (1999). It's the architecture, Mr. Chairman. Retrieved Aug 2004, from http://cyberlaw.stanford.edu/lessig/content/articles/works/cable/Cable.html.

Lewis, J. (2002). *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats.* Washington D.C.: Center for Strategic and International Studies.

Light, L., & Tilsner, J. (1994, Sep 12). Have You Hugged Your Advertiser Today? Retrieved Mar 2007, from http://businessweek.com/archives/1994/b33897.arc.htm.

Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS Quarterly, 16*(2), 173-187.

Loch, K. D., & Conger, S. (1996). Evaluating Ethical Decision Making and Computer Use. *Communications of the ACM, 39*(7), 74-83.

Lohr, S. (2004, Oct 4). I.B.M. Updates Old Workhorse to Use Linux. *The New York Times*. Retrieved Dec 2006, from http://www-306.ibm.com/software/htp/tpf/images/TPF_NYTimes.pdf.

_____. (2007, Mar 5). Time Change a 'Mini-Y2K' in Tech Terms. Retrieved Mar 2007, from http://www.nytimes.com.

Long, C. L. (1999). A Sociotechnical Perspective on Information Security Knowledge and Attitudes. Unpublished Ph.D., The University of Texas at Austin.

Lorsch, J. W. (1970). Introduction to the Structural Design of Organizations. In G. W. Dalton, Paul R. Lawrence, and Jay W. Lorsch (Ed.), *Organizational Structure and Design* (pp. 1-16). Homewood, IL: Richard D. Irwin, Inc. and The Dorsey Press.

Lounsbury, M. (2001). Institutional Sources of Practice Variation: Staffing College and University Recycling Programs. *Administrative Science Quarterly, 46*, 29-56.

Lounsbury, M., & Ventresca, M. (2003). The New Structuralism in Organizational Theory. *Organization*, 10(3), 457-480.

Lu, A. C.-J. (2003). *International Airline Alliances: EC Competition Law/US Antitrust Law and International Air Transport*: Kluwer Law International.

March, J. G. (1994). *A Primer on Decision Making: How Decisions Happen*. New York: The Free Press.

March, J. G., & Simon, H. A. (1958). *Organizations*. New York: John Wiley and Sons, Inc.

McCormick, J. (2003, May 1). Worldspan: Up, Up and Away. Retrieved Mar 2007, from http://www.baselinemag.com/print_article2/0,1217,a=41673,00.asp.

McCullagh, D., & Broache, A. (2006, Aug 7). Senate ratifies controversial cybercrime treaty. Retrieved May 2007, from http://news.com.com/2100-7348-6102354.html?tag=tb.

McFadden, P. J. (1997). Guarding Computer Data. *Journal of Accountancy*, 184(1), 77–79.

McGuire, D. (2004). House OKs More Jail Time for ID Thieves. Retrieved Jun 2004, from http://www.washingtonpost.com/wp-dyn/articles/A190-2004Jun23.html.

McKinley, W., & Mone, M. A. (2003). Micro and Macro Perspectives in Organization Theory: A Tale of Incommensurability. In H. Tsoukas, and Christian Knudsen (Ed.), *The Oxford Handbook of Organization Theory* (pp. 345-372). New York: Oxford University Press.

McKoewn, T. (1998). Why Is A Single Case Important? *APSA-CP Newsletter, 9*(1), 12-15.

McMillan, J. (2006, Sep 29). Interview by author. Atlanta, GA.

Meeting of the Business Roundtable Information Security Coordinating Committee. (2003, Sep 4). Retrieved Apr 2007, from http://www.businessroundtable.org/pdf/1015.pdf.

Meier, K. J., & Bohte, J. (2000). Ode to Luther Gulick: Span of Control and Organizational Performance. *Administration & Society*, 32(2), 115-138.

Merton, R. K. ([1940] 1957/1968). Bureaucratic Structure and Personality. In R. K. Merton (Ed.), *Social Theory and Social Structure*. New York: The Free Press.

Meyer, J. W., Boli, J., & Thomas, G. M. (1994). Ontology and Rationalization in the Western Cultural Account. In Scott, W. R., & Meyer, J. W. (1994), *Institutional Environments and Organizations: Structural Complexity and Individualism*. Thousand Oaks, CA: Sage Publications.

Meyer, J. W., & Rowan, B. (1977). Institutional Organizations: Formal Structure as Myth and Ceremony. *American Journal of Sociology*, 83, 340-363.

Mezias, S. J. (1990). An Institutional Model of Organizational Practice: Financial Reporting at the Fortune 200. *Administrative Science Quarterly*, 35(3), 431-457.

Miles, R. E., Snow, C. C., & Pfeffer, J. (1974). Organization-Environment: Concepts and Issues. *Industrial Relations, 13*(3).

Milton Mueller Delivers Gerbner Lecture 2000. (2000, Summer). *News-link: The Annenburg School for Communication*, University of Pennsylvania, p. 8.

Mitchell, T. (2005, Dec 8). Interview by author. Atlanta, GA.

Mitnick, K. D., Simon, W. L., & Wozniak, S. (2002). *The Art of Deception: Controlling the Human Element of Security*. New York: John Wiley & Sons, Inc.

MIT's Weill on Leveraging Infrastructure. (2003, Jan 21). Retrieved May 2007, from http://www.cioinsight.com/article2/0,1397,838337,00.asp.

Moorman, R. W. (2004). The MRO solution: Airlines are adopting complex software solutions to streamline their maintenance departments. *Air Transport World, 41*(1), 54-57.

Mullin, L. F. (2000, Oct 9). Mullin: FY2000 a year of 'excellent progress'. *Delta NewsDigest, 7,* 7.

_____. (2001, Oct 11). Remarks to the Alabama Business Hall of Fame. Retrieved Jun 2003, from http://www.delta.com/docs/LFM_AL1011.doc.

_____. (2003, Sep 15). Remarks to the International Economic Development Council. Retrieved Jan 2004, from http://www.delta.com/inside/investors/corp_info/speeches/corp_speeches_03/lfm_iedc_2003.html.

_____. (2004, Jan 27). Interview by author, Atlanta, GA.

Murray, C., & Cox, C. B. (2004a). *Apollo 13*. Burkittsville, MD: South Mountain Books.

_____. (2004b). Apollo 13: The crisis begins. Retrieved May 2007, from http://www.apollostory.com/voices/a6.htm.

Murray, J. (2002). Delta powered by IT. *Aircraft Economics*, 1.

Murray, W. H. (1998). Foreword. In D. B. Parker (Ed.), *Fighting Computer Crime: A New Framework for Protecting Information*. New York: John Wiley & Sons, Inc.

Neuman, W. L. (2000). *Social Research Methods: Qualitative and Quantitative Approaches* (4th ed.). Boston: Allyn and Bacon.

Neuman, W. R., McKnight, L., & Solomon, R. J. (1998). *The Gordian Knot: Political Gridlock on the Information Highway*. Cambridge, MA and London: The MIT Press.

Neumann, P. G., & McCullagh, D. (1999). Risks of *Y2K*. *Communications of the ACM*, 42(6), 144.

Nolan, R., & McFarlan, F. W. (2005). Information Technology and the Board of Directors. *Harvard Business Review, 83*(10), 96-106.

North, D. C. (1992a). *The New Institutional Economics and Development (John R. Commons lecture)*. Paper presented at the American Economic Association. Retrieved May 2007, from http://www.econ.iastate.edu/tesfatsi/NewInstE.North.pdf.

_____. (1992b). Institutions and Economic Theory. *American Economist, 36*(1), 3-6.

Nowak, S. (2004, Apr 7). Interview by author. Atlanta, GA.

Odlyzko, A. M. (1998). Smart and Stupid Networks: Why the Internet is like Microsoft. *ACM netWorker*, 2(5), 38-46.

On-time fix requires cross-divisional commitment. (1997, Oct 10). *Delta NewsDigest, 4,* 10-11.

Orru, M., Biggart, N. W., & Hamilton, G. G. (1991). Organizational Isomorphism in East Asia. In W. W. Powell & P. J. DiMaggio (Eds.), *The New Institutionalism in Organizational Analysis (*pp. 361-389). Chicago: The University of Chicago Press.

Osborn, P. (2003, May 12). Cyber-crime Costs $1.5 trillion. Retrieved May 2003, from http://australianit.news.com.au/articles/0,7204,6420661%5E15342%5E%5Enbv%5E15306-15319,00.html.

Ouellette, T. (1996, Dec 2). Delta relies on IBM's MQSeries to tie systems. *Computerworld, 30,* 53.

Overby, S. (2003, Feb 15). The Incredible Lateness of Delta. *CIO Magazine* Retrieved Aug 2006, from http://www.cio.com/archive/021503/infrastructure.html.

Parker, D. B. (1998). *Fighting Computer Crime: A New Framework for Protecting Information.* New York: John Wiley & Sons, Inc.

Peace, G. A., Galletta, D. F., & Thong, J. Y. L. (2003). Software Piracy in the Workplace: A Model and Empirical Test. *Journal of Management Information Systems*, 20(1), 153-177.

Pennings, J. M. (1975). The Relevance of the Structural-Contingency Model for Organizational Effectiveness. *Administrative Science Quarterly*, 20(3), 393-410.

Perrow, C. (1984). *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books.

Petroski, H. (1994). *Design Paradigms: Case Histories of Error and Judgment in Engineering*. Cambridge: Cambridge University Press.

Petzinger, T., Jr. (1996). *Hard Landing: The Epic Contest for Power and Profits That Plunged the Airlines into Chaos*. New York: Three Rivers Press.

Pfeffer, J., & Salancik, G. R. (1977). Organizational Design: The Case for a Coalitional Model of Organization. *Organizational Dynamics, 6*(2), 15-29.

_____. ([1978] 2003). *The External Control of Organizations: A Resource Dependence Perspective*. Stanford, CA: Stanford University Press.

Philips, D. H. (2000, Jul) ADS-B, Automatic Dependent Surveillance – Broadcast: Will ADS-B increase safety and security for aviation? Retrieved May 2007 from http://www.airsport-corp.com/adsb2.htm.

Powell, J. E. (1961). The Water Tower Speech. Retrieved May 2007, from http://www.mdx.ac.uk/WWW/STUDY/xpowell.htm.

Powell, W. W. (1991). Expanding the Scope of Institutional Analysis. In W. W. Powell & P. J. DiMaggio (Eds.), *The New Institutionalism in Organizational Analysis* (pp. 183-203). Chicago and London: The University of Chicago Press.

Powell, W. W., & DiMaggio, P. J. (Eds.). (1991). *The New Institutionalism in Organizational Analysis*. Chicago, Ill.: The University of Chicago Press.

Ragin, C. C. (1987). *The Comparative Method: moving beyond qualitative and quantitative strategies*. Berkeley, CA: University of California Press.

Reed, M. (2003). The Agency/Structure Dilemma in Organization Theory: Open Doors and Brick Walls. In H. Tsoukas & C. Knudsen (Eds.), *The Oxford Handbook of Organization Theory*. New York: Oxford University Press.

Reuters News Service. (2004, Apr 30). UPDATE 2-Delta names new chief financial officer. Retrieved Apr 2007, from http://www.forbes.com/newswire/2004/04/30/rtr1355053.html.

Richardson, R. (2004). 2004 CSI/FBI Computer Crime and Security Survey. Retrieved Oct 2004, from http://www.gocsi.com/awareness/fbi.jhtml;jsessionid=HQHZR0MLEPH02QSNDBCSKHSCJUMEKJVN.

Rittel, H. & M. Webber. (1973). Dilemmas in a General Theory of Planning. *Policy Sciences*, 4, 155-169.

Robb, C. (2004, Apr 13, 21). Interview by author. Atlanta, GA.

Rosencrance, L. (2004, Jan). Computer containing airline ticketing info stolen. Retrieved May 2007, from http://www.computerworld.com/securitytopics/security/story/0,10801,89062,00.html.

Ross, J. W. (2001, Aug). E-Business at Delta Air Lines: Extracting Value from a Multi-faceted Approach. Retrieved Apr 2006, from http://web.mit.edu/cisr/www/html/jwr_cases_2.html.

Rothfeder, J. (2005, Feb 5). Can Information Technology Save the Airlines? Retrieved Aug 2006, from http://www.cioinsight.com/article2/0,1540,1765191,00.asp.

Sabel, C. F. (1982). *Work and Politics: the Division of Labour in Industry*. Cambridge: Cambridge University Press.

Safranski, M. (2005, Jul 20). Comments: OODA Loop as Flowchart, Try 2. Retrieved Apr 2007, from http://www.tdaxp.com/archive/2005/07/20/ooda-loop-as-flowchart-try-2.html.

Sagan, S. D. (1993). *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons*. Princeton, N.J.: Princeton University Press.

Sager, I., & Greene, J. (2002, Mar 18). The Best Way To Make Software Secure: Liability. *Business Week*, 61.

Saia, R. (1999, Jun 28). In Command of Y2K *Computerworld,* 54.

Scalet, S. D. (2003, Jan). Cleared for Takeoff. Retrieved Aug 2006, from http://www.csoonline.com/read/010903/takeoff.html.

Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*. New York: Wiley Computer Publishing.

_____. (2003). *Beyond Fear*. New York: Copernicus Books.

_____. (2007, Feb 28). The Psychology of Security *Crypto-Gram Newsletter* Retrieved Apr 2007, from http://www.schneier.com/crypto-gram-0702a.html.

Schoonhoven, C. B. (1981). Problems with Contingency Theory: Testing Assumptions Hidden within the Language of Contingency "Theory." *Administrative Science Quarterly, 26*, 349-377.

Schultz, E. E. (2002). A Framework for Understanding and Predicting Insider Attacks. *Computers & Security*, 21(6), 526-531.

Scott, W. R. (1987). The Adolescence of Institutional Theory. *Administrative Science Quarterly*, 32, 493-511.

_____. (1992). *Organizations: Rational, Natural, and Open Systems* (3rd ed.). Englewood Cliffs, N.J.: Prentice Hall.

_____. (1995). Introduction: Institutional Theory and Organizations. In W. R. Scott & S. Christensen (Eds.), *The Institutional Construction of Organizations: International and Longitudinal Studies* (pp. xi-xxiii). Thousand Oaks, CA: Sage Publications.

_____. (2000, Apr 28-30). *Organizations and the Natural Environment: Evolving Models.* Paper presented at the Organizations, Policy, and the Natural Environment: Institutional and Strategic Perspectives Evanston, IL.

_____. (2001). *Institutions and Organizations* (2nd ed.). Thousand Oaks, CA: Sage Publications.

_____. (2004). Reflections on a Half-Century of Organizational Sociology. *Annual Review of Sociology*, 30, 1-21.

Scott, W. R., & Christensen, S. (Eds.). (1995). *The Institutional Construction of Organizations: International and Longitudinal Studies*. Thousand Oaks, CA: Sage Publications.

Scott, W. R., & Meyer, J. W. (1983). The Organization of Societal Sectors. In J. W. Meyer & W. R. Scott (Eds.), *Organizational Environments: Ritual and Rationality* (pp. 129-154). Beverly Hills, CA: Sage Publications.

_____. (1994). *Institutional Environments and Organizations: Structural Complexity and Individualism*. Thousand Oaks, CA: Sage Publications.

Scott, W. R., Ruef, M., Mendel, P. J., & Caronna, C. A. (2000). *Institutional Change and Healthcare Organizations: From Professional Dominance to Managed Care.* Chicago and London: The University of Chicago Press.

Seidenman, P., & Spanovich, D. (2004, Dec 7). Airlines Spending Money on IT. *Overhaul & Maintenance*.

Selznick, P. (1948). Foundations of the Theory of Organization. *American Sociological Review, 13*, 25-35.

_____. (1957). *Leadership in Administration: A Sociological Interpretation*. Berkeley, Los Angeles, and London: University of California Press.

_____. (1996). Institutionalism 'Old' and 'New'. *Administrative Science Quarterly, 41*(2), 270-278.

Shackford, K. M., & Shackford, J. E. (2003). *Charting a Wiser Course: How Aviation Can Address the Human Side of Change*. Incline Village, Nevada: The Mattford Group Press.

Shinal, J. (2006, Aug 18). Security technology trumped by other concerns. Retrieved Aug 2006, from http://www.marketwatch.com/News/Story/Story.aspx?dist=newsfinder&siteid=mktw&guid=%7BDD167595%2DF82B%2D4D46%2DB48F%2D6ECD1F867A58%7D&.

Shtern, E. (2007). Interview by author, Atlanta, GA.

Sills, D. L. (1970). Preserving Organizational Goals. In O. Grusky, and George A. Miller (Ed.), *The Sociology of Organizations: Basic Studies.* New York: The Free Press.

Simon, H. A. ([1945] 1976). *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organization*. (3rd ed.). New York: Free Press.

Slater, D. (1998, Jan 15). The Hidden Costs of ERP Software: ERP software packages-SAP's R/3, Baan, PeopleSoft and their ilk-promise great benefits. But exactly how much will you have to pay to get them? Retrieved Mar 2007, from http://www.cio.com/archive/enterprise/011598_erp.html.

Smart, E. (1999, Sep 28). Will Y2K Snarl Global Transportation? Retrieved Aug 2004, from http://www.senate.gov/~y2k/hearings/990930/smart.htm.

Smith, A. ([1776] 1985). *An Inquiry into the Nature and Causes of the Wealth of Nations*. New York: Random House.

_____. ([1776] 1996). On the Division of Labor. In J. M. Shafritz, & J.F. Ott (Ed.), *Classics of Organization Theory* (4th ed.). Fort Worth, TX: Harcourt Brace College Publishing.

Smithsonian National Museum of American History. Terminal Interchange from PANAMAC Airlines Reservation System. Retrieved Aug 2006, from http://americanhistory.si.edu/collections/object.cfm?key=35&objkey=33.

_____. Transportation Technology, 1950-2000. Retrieved Mar 2007, from http://americanhistory.si.edu/onthemove/themes/story_50_1.html.

Sofaer, A. D., Grove, G. D., & Wilson, G. D. (2001). Draft International Convention to Enhance Protection from Cyber Crime and Terrorism. In A. D. Sofaer & S. E. Goodman (Eds.), *The Transnational Dimension of Cyber Crimes and Terrorism:* The Hoover Institution on War, Revolution and Peace.

Stackpole, B. (1994). AT&T/Delta deal redefines outsourcing; will offer IS services to others in transportation. *PC Week, 11*(35).

Staying the Course. (2003, Feb 15). *CIO magazine*. Retrieved Sep 2006, from http://www.cio.com/archive/021503/infrastructure_sidebar_1.html.

Stinchcombe, A. L. (1965). Social Structure and Organizations. In J. G. March (Ed.), *Handbook of Organizations* (pp. 142-193). Chicago: Rand McNally.

_____. (1997). On the Virtues of the Old Institutionalism. *Annual Review of Sociology,* 23, 1-18.

Straub, D. W. Jr., (1990). Effective IS Security: An Empirical Study. *Information Systems Research*, 1(3), 255-276.

Straub, D. W., Jr., & Nance, W. D. (1990). Discovering and Disciplining Computer Abuse in Organizations: A Field Study. *MIS Quarterly, 14*(1), 45-60.

Straub, D. W., Jr., & Welke, R. J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision-Making. *MIS Quarterly, 22*(4), 441-469.

Taylor, F. W. ([1916] 1996) The Principles of Scientific Management. In J. M. Shafritz & J. F. Ott (Eds.), *Classics of Organization Theory*. Chicago: Dorsey Press.

Taylor, J. R. (2001). The "Rational" Organization Reconsidered: An Exploration of Some of the Organizational Implications of Self-Organizing. *Communication Theory*, 11(2), 137-177.

Taylor, W. (2004, Apr 7). Interview by author. Atlanta, GA.

Technology Leadership: Delta Technology. (2004, Feb) *Air Transport World*, 41.

Thompson, J. D., Zald, M. N., & Scott, W. R. ([1967] 2003). *Organizations in Action: Social Science Bases of Administrative Theory*. New Brunswick and London: Transaction Publishers.

Tillquist, J. (2002). Rules of the game: constructing norms of influence, subordination and constraint in IT planning. *Information and Organization, 12*, 39-70.

Turner, B. M. (1976). The Organizational and Interorganizational Development of Disasters. *Administrative Science Quarterly, 21*, 378-397.

U.S. Department of Justice. (1998, May 22). Policy on Critical Infrastructure Protection: Presidential decision directive 63. Retrieved May 2007 from http://www.usdoj.gov/criminal/cybercrime/white_pr.htm.

_____. (2003, Nov 10). Council of Europe Convention on Cybercrime. Retrieved May 2007, from http://www.usdoj.gov/criminal/cybercrime/COEFAQs.htm#QA5.

U.S. Government Accountability Office. (2006, Sep). Information Security: Coordination of Federal Cyber Security Research and Development. Retrieved May 2007, from http://www.gao.gov/new.items/d06811.pdf.

Van de Ven, A. H., & Delbecq, A. (1974). The Effectiveness of Nominal, Delphi, and Interacting Group Decision-making Processes. *Academy of Management Journal, 17*(4), 605-621.

Varian, H. R. (2000). Managing Online Security Risks. Retrieved Oct 2004, from http://www.nytimes.com/library/financial/columns/060100econ-scene.html.

Vaughan, D. (1990). Autonomy, Interdependence, and Social Control: NASA and the Space Shuttle *Challenger*. *Administrative Science Quarterly, 35*, 225-257.

_____. (1999). The Dark Side of Organizations: Mistake, Misconduct, and Disaster. *Annual Review of Sociology, 25*(1), 271-305.

Verton, D. (2004, Apr 9). TSA to Launch Registered Traveler Program: Biometrics Will Speed Frequent Fliers through Security Checkpoints. Retrieved Apr 2004, from http://www.computerworld.com/printthis/2004/0,4814,92099,00.html.

Vijayan, J. (2006, Dec 13). Vermont officials blast contractor for security lapse: Social Security numbers of health care providers were posted online. *Computerworld* Retrieved Dec 2006, from http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9005940&source=NLT_SEC&nlid=38.

Violino, B. (1992, Jul 6). Maintenance on the MARC. (Delta Air Lines Inc.'s Maintenance & Rebuild Control automation project). *InformationWeek*.

Wagner, J. (2004, Dec 27). Comair Back in Air After Computer Outage. Retrieved Feb 2007, from http://www.internetnews.com/bus-news/article.php/3451981.

Weber, M. ([1906-1924] 1946 / 1958). Bureaucracy (H. H. Gerth & C. W. Mills, Trans.). In H. H. Gerth & C. W. Mills (Eds.), *From Max Weber: Essays in Sociology*. New York: Oxford University Press.

_____. ([1924] 1968). *Economy and Society: An Interpretive Sociology* (G. Roth & C. Wittich, Eds.). New York: Bedminister Press.

_____. (1970). Bureaucracy. In O. Grusky & G. A. Miller (Eds.), *The Sociology of Organizations: Basic Studies* (pp. 5-23). New York: The Free Press.

Weiss, T. R. (2004, May 03). Brief: Delta Air Lines flights canceled, delayed due to computer glitch. Retrieved May 2007, from http://www.computerworld.com/industrytopics/travel/story/0,10801,92857,00.html.

Werbach, K. (1997). *Digital Tornado: The Internet and Telecommunications Policy* (OPP Working Paper Series). Washington, D.C.: FCC Office of Plans and Policy.

Westby, J. (Ed.). (2007). *Outsourcing Risk Management*: American Bar Association.

Whitman, M. E. (2004). In Defense of the Realm: Understanding the Threats to Information Security. *International Journal of Information Management, 24*(1), 43-57.

Who We Are. (2004, Apr). Retrieved Apr 2007, from http://www.postnormaltimes.net/blog/html/about.html.

Will, G. (2003, Feb 18). Delta Breaks Into Song. Retrieved Aug 2006, from http://www.jewishworldreview.com/cols/will021803.asp.

Williamson, M. (1997, Jul 1). Strategic Planning: For Richer, For Poorer. Retrieved Jun 2006, from http://www.cio.com/archive/070197/strategic.html.

Williamson, O. E. (1995). Transaction Cost Economics and Organization Theory. In O. E. Williamson (Ed.), *Organization Theory: From Chester Barnard to the Present and Beyond* (pp. 207-256). New York and Oxford: Oxford University Press.

Wilson, J. Q. (1991). *Bureaucracy: What Government Agencies Do and Why They Do It*. New York: Basic Books.

Wood, C. C., & Banks, W. W., Jr. (1993). Human Error: An Overlooked but Significant Information Security Problem. *Computers & Security, 12*(1), 51-60.

Woodfill, J. (2004, Nov). Apollo 13 "Houston, we've got a problem." Retrieved May 2007, from http://www1.jsc.nasa.gov/er/seh/pg2.htm.

Woods, W. (2002, Feb 4). Flight attendants accuse Delta of intimidation in failed union vote Retrieved Mar 2007, from http://www.lraonline.org/story.php?id=225.

Woodward, J. (1970). Technology and Organization. In O. Grusky, and George A. Miller (Ed.), *The Sociology of Organizations: Basic Studies*. New York: The Free Press.

Wrolstad, J. (2003). I.T. Chiefs Form Security Council. Retrieved May 2004, from http://enterprise-security-today.newsfactor.com/story.xhtml?story_id=22686.

Y2K. (1999). *Journal of Business Strategy*, 20(2).

Yin, R. K. (1982). Studying Phenomenon and Context across Sites. *American Behavioral Scientist, 26*(1), 84-100.

_____. (1994). *Case Study Research: Design and Methods* (2nd ed. Vol. 5). Thousand Oaks, CA: Sage Publications.

_____. (2003). *Applications of Case Study Research* (2nd ed. Vol. 34). Thousand Oaks, CA: Sage Publications.

Yourdon, E. (2000, Jan 24). *Y2K* Success Lessons. Retrieved Sep 2004, from http://www.computerworld.com/news/2000/story/0,11280,40853,00.html.

Zucker, L. G. (1987). Institutional Theories of Organization. *Annual Review of Sociology, 13*, 443-464.

VITA

PAMELA GRACE BURNS HASSEBROEK

Pam Hassebroek was born in Sherman, Texas, U.S.A., a small town in north central Texas where she attended kindergarten and first grade in private settings, and public schools from second grade through high school. Growing up on a dairy farm during her childhood provided another dimension of her education. Hassebroek witnessed first hand the changes from an agrarian society to industrial and then to an information society in America. During that time, along with her family, she experienced the struggles of farmers who found it increasingly difficult to stay in business as sole proprietors and to remain landowners. Profit margins on hard-earned farm products were continuing to erode while the lands were of increasing interest to commercial pursuits.

Following graduation from Sherman High School, Hassebroek received a Bachelor of Arts degree in Mathematics from Texas Christian University, and holds Master of Science degrees from two institutions. She earned the M.S. in Petroleum Engineering from The University of Texas at Austin, and the M.S. in Digital Media from the Georgia Institute of Technology. She achieved the credential of Registered Professional Engineer while employed at Exxon Production Research Company in Houston, Texas.

Hassebroek's extensive career comprises three phases. First, in research and staff positions in major oil companies she employed numerical simulation techniques and the power of supercomputers to optimize the exploitation of petroleum reservoirs. The extreme expense and high technology equipment and skills required to perform these studies led to their application only to the great petroleum reservoirs around the globe. She analyzed aspects of exploitation and production of reservoirs in the U.S., the Arabian Peninsula, the North Sea, and Canada.

In the second phase, Hassebroek worked as a developer, teacher, and administrator of curricula for IT instruction in the K-12 schools where her children were students. This career phase included employment at St. John's School in Houston, Texas, at Taipei American School in Taipei, Taiwan, and at the Lovett School in Atlanta, Georgia.

In the third and current phase, her coursework and research at Georgia Tech (GT) has focused on the social consequences of information technology (IT), which has given her a strong academic foundation for this dissertation. Along with other experiences at GT—in independent study, in various research and teaching assistantships, she has assisted in teaching and in the course development process for the Georgia Tech Information Security Center (GTISC).

Hassebroek has written about, formally presented, and published aspects of her research in a variety of venues in the U.S., Europe, and the Middle East. She has received awards for her work from Cisco Systems, the U.S.-based company that designs and sells networking and communications technology and services worldwide, and from (ISC)²®, the globally recognized organization for certifying information security professionals. In the fall of 2004, the Sherman High School Ex-students Association recognized her as a distinguished graduate; and in 2004/2005, the Georgia Institute of Technology School of Public Policy honored her as the Outstanding Ph.D. Student.